UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

DATA DRIVEN NETWORK DESIGN FOR CLOUD SERVICES BASED ON HISTORIC UTILIZATION

A THESIS

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

Degree of

MASTER OF SCIENCE IN ELECTRICAL & COMPUTER ENGINEERING

By

DAVID BUTCHER
Norman, Oklahoma
2022

DATA DRIVEN NETWORK DESIGN FOR CLOUD SERVICES BASED ON HISTORIC UTILIZATION

A THESIS APPROVED FOR THE
ELECTRICAL & COMPUTER ENGINEERING DEPARTMENT

BY THE COMMITTEE CONSISTING OF

Dr. James Sluss, Chair

Dr. Ali Imran

Dr. Samuel Cheng

Table of Contents

List of Tables

List of Figures

Abstract

In recent years we have seen a shift from traditional networking in enterprises with Data Center centric architectures moving to cloud services. Companies are moving away from private networking technologies like MPLS as they migrate their application workloads to the cloud. With these migrations, network architects must struggle with how to design and build new network infrastructure to support the cloud for all their end users including office workers, remote workers, and home office workers. The main goal for network design is to maximize availability and performance and minimize cost. However, network architects and network engineers tend to over provision networks by sizing the bandwidth for worst case scenarios wasting millions of dollars per year. This thesis will analyze traditional network utilization data from twenty-five of the Fortune 500 companies in the United States and determine the most efficient bandwidth to support cloud services from providers like Amazon, Microsoft, Google, and others. The analysis of real-world data and the resulting proposed scaling factor is an original contribution from this study.

I. Introduction

There has been a paradigm shift in recent years with information technology services moving to the cloud. GlobalData forecasts the market in the U.S. to exceed $233 billion dollars by 2025 with a compound annual growth rate of 12.9% [1]. Large multi-national corporations (MNCs) accustomed to data center centric environments and private networks must evaluate migrating to cloud services. Assurance of end-to-end quality of experience is of high importance for business-critical applications. According to a worldwide survey of over 3700 companies conducted in 2020, businesses adopting cloud services are primarily concerned with reliability, while performance ranks third on the list of concerns [108]. Applications are the driving force behind the MNCs connectivity needs and many vendors are pushing customers toward a software-as-a-service (SaaS) model. The SaaS model provides a full application environment providing hardware, software, and availability in the cloud allowing a pay per use model. This presents an opportunity for MNCs to reevaluate their network environments determining the best model to support their business whether private cloud, public cloud, or hybrid cloud.

For practical discussion, private cloud is defined as private connectivity like multi-protocol label switching (MPLS) or layer 2 Ethernet into a collocation facility or customer owned data center facility with dedicated hardware resources per customer. Public cloud would be Internet based connectivity into a service provider's facility or data center with shared hardware resources and virtual environments per customer. Hybrid cloud is a combination of both with resources in private facilities and service provider facilities with private and Internet based connectivity for application access from both dedicated and shared hardware resources.

Whether private, public or hybrid, the cloud is based on virtualization. Virtualization technologies simplify IT infrastructure by breaking the close association between applications and specific hardware resources. Virtualization allows decoupling of computing hardware from applications and management systems. Hardware and software can follow independent evolutionary paths since changes to one can have minimal effect on the other. Virtualization provides a new abstraction layer which defines the possible interactions with hardware [88]. It makes it possible to deploy applications on a working set of servers taken from a generic pool which is capable of supporting many applications. It also makes it possible to move applications between servers in the pool and add or remove servers dynamically. This means the infrastructure can respond to changes in demand, failure of server hardware, or changes in network connectivity. Virtualized computing offers the flexibility to define dynamic virtual environments with its own application specific context for access control, encryption, monitoring, logging, queuing, scheduling, etc.

The cloud environments offer several services including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), Unified Communication-as-a-Service (UCaaS), Storage-as-a-Service (STaaS), and many others on a pay per use basis. Cloud environments typically offer a web portal to setup and configure the virtual services companies require, including hardware only and full software stacks. The services offered reduce or even eliminate the need for companies to own, operate, and maintain their own data centers. Many vendors MNCs use to run their business including Microsoft, Cisco, Oracle, IBM, HP, Amazon, Google, and others are pushing their customers toward these services. One of the issues with migration for network architects and engineers is determining the required bandwidth for efficient connectivity to the cloud.

Primary connectivity for the cloud is based on the Internet. The Internet first began in October 1969 with the first large scale packet switching network known as ARPAnet [72]. The basic protocol of the ARPAnet was NCP, which combined addressing and transport into a single protocol [73]. NCP was not very reliable. As a result, reliability was separated from addressing and packet transfer in the design of the Internet protocol suite, and IP was separated from TCP. The switchover to TCP/IP culminated in January 1983, when ARPAnet officially became the Internet [72]. In 1982 the domain name system (DNS) was deployed to replace original hosts.txt files for naming Internet systems [74]. This was a clear response to a scaling problem, and DNS solved the issue of distributing files of host names and decentralized the administration of the namespace.

Link-state routing protocols were developed as a direct response to the convergence problems suffered by distance-vector routing protocols as the Internet grew in size [75]. The Exterior Gateway Protocol (EGP) was a direct response to the scaling limitations of intra-domain routing, allowing routing within a network to be isolated from routing between networks [76]. With EGP came the need for policy routing, where each network could decide for itself which routes to use and to propagate to other networks, while the network as a whole still maintained routing integrity [72]. The Border Gateway Protocol (BGP) was the result and has been used for inter-domain routing ever since [77].

For over 25 years BGP has provided inter-domain routing for the Internet [78]. BGP is conceptually very simple. Routes to subnets are advertised together with attributes of the path to that subnet. These attributes include the path of routing domains that the route has taken through the network. Each time an AS passes on a route to another AS, it adds its own AS number to the AS path contained in the route. BGP's goal is to enable policy routing, where each routing domain can make its own choice about which routes to accept from its neighbors and which routes to pass on to other neighbors. BGP is slow to converge, error prone, easy to misconfigure, difficult to debug, and insecure [72]. BGP is the most critical piece of the Internet, and if it ever failed it would be very painful for millions of businesses around the world.

Classless Inter-domain Routing (CIDR) was introduced in 1993, and the Internet transitioned from academic to a commercial network [72]. One of the main drivers of this transition was the World Wide Web (WWW), which started in 1993 with the NCSA Mosaic web browser. Since 1993, there haves been small tweaks, but no significant changes to the core protocols that form the basis of the Internet. The Internet was never designed to be optimal for any particular problem. Its great strength is that it is a general-purpose network that can support a wide range of applications and a wide range of link technologies. The Internet is also a cost-effective network, but it does not make promises about the quality of service it provides. Three decades later and millions of wireless devices joining the wired, we find ourselves transitioning to the cloud on the same Internet.

Now, we must determine the Internet bandwidth required at each site. Many variables are involved in determining the required bandwidth for a given location including situations with the workforce such as work patterns of users, time spent in meetings, time on the phone, remote work away from the office, vacation and sick time, shift work and breaks, etc. Since there are so many unknowns, the problem with defining bandwidth requirements can be seen as nondeterministic polynomial time hard (NP-hard). It is very challenging and sometimes impossible to develop an algorithm to solve NP-hard problems. Network architects and engineers will typically only address concrete terms in their calculations including required bandwidth per application and number of users per site to get a required bandwidth per site.

One of the goals when designing a network is to maximize performance and availability and minimize cost [2]. Using only known variables in the calculations can result in networks being over provisioned for bandwidth, thus wasting operating capital resources. In many situations architects and engineers design networks for "rainy day" or "worst case scenario" missing the goal to minimize cost. This study offers one possible solution to this problem by analyzing existing utilization data from real world network environments and using the analysis to determine the bandwidth needs for cloud services. In addition, the study examines a traditional bandwidth design formula and suggests a scaling factor be added to the calculations to build efficient network environments for the cloud.

Through the literature review no other works were found using real-world utilization data from twenty-five Fortune 500 companies to determine efficient bandwidth for cloud services. In addition, no other work has proposed a scaling factor for calculating bandwidth. Therefore, the analysis of real-world data from twenty-five companies and the proposed scaling factor is an original contribution from this study.

The twenty-five companies selected for analysis include some of the largest MNCs in banking and finance, retail, oil and gas, home building, insurance, and consumer services. Over 29,000 circuits were analyzed during a 12-month period on existing MPLS networks with company owed data centers. The idea is all companies will maintain the same applications from their current environments and migrate to cloud service providers like Amazon, Microsoft, Google, and others. The new data centers will be provided by the cloud service providers and the networks will be Internet based including dedicated Internet, broadband, and wireless. Dedicated Internet service would consist mainly of Ethernet over fiber access, broadband would consist of DSL, Cable, or fiber passive optical networks (PONs), and wireless would consist of long-term evolution (LTE 4G) and new radio 5G (NR-5G). Mobility will play a large role as companies migrate to the cloud, especially from a mobile edge computing (MEC) standpoint.

However, the data was not available for analysis, so MEC utilization was not included in this work.

All companies analyzed had class of service (COS) configured on their MPLS circuits for critical latency sensitive applications like IP voice and IP video. As these organizations plan to migrate to the cloud it would be prudent to work with Internet service providers offering COS or investigate architectures such as software define wide-area-networks (SD-WANs). SD-WAN would allow the provisioning of tunnels between the sites and COS policies can be configured for the traffic traversing the tunnels. This would require SD-WAN equipment or virtual machines (VMs) in the cloud service providers data center or collocated in a data center offering cloud exchange services to access all cloud service providers.

Many of the circuits analyzed for each of the companies were part of diverse pairs providing diverse paths, central offices (COs), points-of-presence (POPs), and customer premise equipment. The circuits had bi-directional forwarding detection (BFD) configured at layer 2 of the protocol stack to detect any anomalies between the customer edge routers and the provider edge routers. At layer 3, routing protocols like border gateway protocol (BGP) were configured for diversity to primary and backup data centers. The diversity requirements for these sites would remain the same, so a cloud design would include these elements relying on the cloud service providers to provide redundancy between their data centers for critical application availability. An interesting survey was done for managing these types of complex environments and equipment configuration was a primary concern [80]. 49.8% of respondents ranked “check the config” as their top concern for change management and “make the config” as their second concern. The command line interface (CLI) is used in 50% of router/switch configurations, and a graphical user interface (GUI) is used in 60% of firewall/load balancer/IDS configurations

[79]. In the future, virtualization could possibly impact this and configuration with a GUI will probably increase. The intuitive GUI design can certainly improve work efficiency for novice engineering team members.

The current environment for the companies analyzed is a private network infrastructure with company owned data centers free from the attacks of the Internet. As the companies move to Internet based connectivity they will have to deal with phishing, viruses, malware, denial of service, and other security risks associated with the cloud. If the network security is not designed properly, it could have a negative impact on bandwidth requirements. Denial of service and distributed denial of service attacks are designed to saturate connections with tremendous amounts of traffic driving the utilization on Internet circuits to maximum amounts making the connections unusable. Security is not a specific focus of this work, but it is critical for successful cloud migration being a topic for further discussion on how it impacts bandwidth utilization.

The analysis of the data has shown all twenty-five Fortune 500 companies have networks over provisioned. The goal to minimize cost in all companies has not been met. The data shows financial resources are being wasted on connectivity instead of research, product development, engineering, or other areas to make the companies more productive, efficient, and profitable. As these companies migrate to cloud services, they have the opportunity to improve their network efficiency by right-sizing bandwidth needs. This study focuses on the analysis of current network utilization using historic data to offer a roadmap to cloud migration.

The remainder of this thesis is organized as follows. Chapter II provides a literature review on network design. Chapter III specifies the methodology used for gathering and analyzing the current utilization data. Chapter IV presents the results and explanation for the analysis, and Chapter V offers the conclusions and discussion for future work.

II. Literature Review

A. Models in Network Design

The concept of using historical data to determine efficient cloud migration is a unique idea determined after reviewing many concepts from the literature on network design. Many within the networking community advocate that engineers should use common realistic models [3]. However, no model exists which can be applied to every possible networking problem. George E.P. Box, a British statistician, once said, “All models are flawed, some are useful.” For networking models, it is important to identify the appropriate timescale to analyze the problem at hand [4]. This is because certain factors only exhibit themselves and influence the system at certain times. At shorter timescales the influencing factors include protocol interactions with hardware and human factors such as how often a user is active. At medium timescales different factors become important with a strong impact made by human behaviors which are influenced by time of day and time of year. At longer timescales the behavior of the network and its traffic are affected by seasonal patterns, long-term growth, and pattern changes due to the emergence of new applications.

In the past, traffic and performance studies had been predominantly based on models such as Poisson processes that have no long-term correlation structure [4]. Such models are attractive because of their mathematical tractability and the large body of queuing theory that relies on the assumption of Poisson processes. The design problems associated with automatic network design are NP-hard and generally beyond formal optimization techniques for realistically sized problems [13]. A pivotal study found evidence of long-range correlation in traffic and brought the concept of self-similarity into the field of network traffic and performance analysis [5]. Self-similarity is described as the property of an object which looks the same when viewed at different scales. For network traffic this can be thought of loosely as the idea the traffic is bursty in the same way whether the timescale is milliseconds or seconds.

Statistical concepts for network traffic define three properties, long-range dependence (LRD), statistical self-similarity, and heavy tails. LRD can be thought of as a correlation persisting over an extremely long period of time and as a significant power in low-frequency bands. A variable is said to be heavy-tailed distributed if the tail of the distribution function decreases to zero more slowly than exponentially [6]. A heavy tailed distribution implies that large values can occur with a non-negligible probability. It has been shown that a superposition of ON/OFF processes where the lengths of ON and OFF periods are heavy tailed will give rise to a self-similar process. It can also be seen that heavy tails in the ON and OFF periods could lead to long-range correlations in the process. Three different studies found that wide-area network (WAN) traffic is consistent with self-similar scaling [7] – [9]. The studies show Poisson processes adequately model certain session arrivals such as FTP and TELNET, but not others such as HTTP, SMTP and NNTP. In addition, self-similarity in Web traffic could be explained by the long-tailed nature of the distribution of file sizes, the effect of user behavior, and the aggregation of multiple flows in the network.

A network model includes topology but also traffic characteristics, congestion levels, protocols, scheduling policies, etc. Floyd and Kohler [3] argue that it is not conceivable to design a unique network model that can be employed in all circumstances and draw meaningful conclusions. Rather, network models should be crafted by the engineer based on the problem at hand to capture the relevant behavior and ignore redundant ones. Paxson and Floyd [7] argue that accurately simulating the Internet is an impossible task as it is a continuously moving target affected by continuous topological, traffic, and routing changes. Under conservative assumptions regarding the number of Internet hosts and their traffic demands, simulating a network the size of the Internet is computationally not tractable. A modeling tool for circuit reliability based on Markov techniques can represent unprotected and protected paths through network elements using fault data to calculate end-to-end service failure rates and availability [13].

B. Service Architecture and Design Elements

Another concept in network design is the service infrastructure architecture such as network, service platform, applications environment, and operational support system (OSS) [10]. The core network is typically a synchronous optical network (SONET) and dense wave division multiplexed (DWDM) transport supporting an MPLS core. Networks are constructed from nodes, subspans, and paths where a node is a flexibility point capable of re-routing blocks of capacity, a subspan is a transmission system connecting two such nodes, and a path is the route traffic takes through the network [13]. This layer is not limited to any technology applying equally well to SONET, WDM, Internet protocol (IP), and software defined networks (SDN). Commonly these layers are designed independently, but the new approach is to consider multiple layers simultaneously during the design process to realize scalability while optimizing cost [53]. The goal is to design the links in an IP layer which are carried as wavelengths over a fixed transport network layer.

There have been some recent developments in the transport network. The developments in digital signal processing combined with coherent detection have already enabled operation at different modulation formats using a single line interface [97]. Coupled with the standardization of a flexible grid and the deployment of bandwidth variable wavelength selective switches at each reconfigurable optical add/drop multiplexor, this makes it possible to effectively trade off capacity by reach and attain spectral efficiencies of up to 5 b/s/Hz [98] - [100]. It becomes possible to transmit 200 Gbps quadrature phase shift keying optical channels over ultra-long-haul networks and 600 Gbps optical channels using 64QAM over short distances for metro interconnection applications [101]. The higher order modulation formats, 32 QAM and 64 QAM, are only available with the next generation of line interfaces and the reach of 64 Gbaud optical channels assume a penalty when compared to 32 Gbaud optical channels using the same modulation format, which is due to operating at a higher symbol rate. The use of this new framework makes it possible to reach higher spectral efficiencies throughout at later stages of the network lifetime without incurring spectrum fragmentation limitations and maintaining the spectral management complexity at lower levels. This efficient management makes it possible to maximize the carried traffic load, which shows the effectiveness of this framework to postpone expensive fiber implementations or leases [101].

Network service delivery is IP-based, and access networks are converged on a multiservice platform. The platform supports fixed mobile converged services and multimedia services on a 3rd Generation Partnership Program IP Multimedia Subsystem (3GPP IMS) for 4G long-term evolution (LTE) and 5G new radio (NR) [11]. The application environment should be designed to support both multimedia and mobile services having interfaces to an open platform exposed to enable third parties to deliver services based on the underlying network [12].

To enable a simple and complete vision, the OSS should be transformed into systems which are part of the service rather than the back-office, converging with the network intelligence. The OSS needs to address the range of IT components and deliver a high grade of flexibility spanning multiple operational domains bringing service providers into a single, integrated environment [52]. Service execution should be a service-oriented architecture defining common services which are exposed as web services in a service assembly environment [10]. The service enablers are functions like session control, authentication, presence, location, and profile providing the necessary tools and support to facilitate the enablers being built into new services. For mobile convergence and integration throughout the network the service execution architecture requires session initiation protocol (SIP) [11]. OSS development should follow the Information Technology Infrastructure Library (ITIL) standards [52].

Enterprise networks consist of IP networks composed of three major subnetworks, access, edge, and core [14]. The access network links the customer premise equipment to the edge routers, the edge network aggregates the traffic flows to the core routers, and the core routers consist of high-speed routers meshed with highspeed links. It is important to select the correct number of routers at each level, the correct port types in each router, and the correct link characterized by technology and rate. The cost function, representing the total cost of the network, is composed of the cost of the links, C_L, the cost of the routers, C_R, and the cost of the ports, C_P [14]. The model for the topological optimization problem of IP networks with a three-level hierarchical structure, denoted P, is given by

$$P = \min_{v,w,x,y,z} C_L(\mathbf{x}, \mathbf{y}, \mathbf{z}) + C_R(\mathbf{v}) + C_P(\mathbf{w})$$

We should focus on the C_L of this equation because in a typical network 40% of the capital investment is in the customer access network [46]. The marginal cost of providing broadband services is dependent on the costs of upgrading the access network migrating to optical fiber technology. C_R and C_P can be combined into node cost [64] and the equation would become

$$\mathrm{CT} = \sum_{i=1}^{n} \mathrm{Ci} + \sum_{i=1}^{n} \sum_{j=1}^{n} \mathrm{Cij}$$

CT is the total cost, Ci is the cost of the network equipment placed at location i, and Cij gives the cost of the link between node i and node j.

The network is built to connect data centers (DCs) serving all the data needs of the enterprise. Thousands of business applications and services are hosted by the DCs and consumed by users, partners, associates, etc. The typical scale of an enterprise DC ranges from 50,000 to 200,000 servers and the application to server ratio ranges from 10 to 1000 servers [15]. Network infrastructure and resources contribute to more than 20% of DC capital expenditure and a major part in the operational expenditure. Network engineers are challenged to develop state-of-the-art networks even though the state-of-the-art is continually changing. Both the novice network designer and the seasoned network architect are mainly concerned about how to design a network that can keep pace with the accelerating changes.

Several factors influence the complexity of the overall network design including IP addressing, scaling, switched LAN design, WAN technology options, resilience, customer application environments, and security [34]. Sun, et al., [69] argue for systematic network design by showing how ad hoc processes result in inconsistencies and do not ensure correctness or lead to better designs. Every device in an enterprise network requires an IP address to uniquely identify it. Users require access to the Internet for cloud service environments, email, web, etc. The growth in Internet use over the years has exhausted registered IPv4 addresses requiring introduction of IPv6 which complicates management of IP addressing schemes. Companies either deploy dual stack IP addressing or deploy network address translation from private to public addressing.

Although an organization may have a vast range of private IP addresses for use, it is still important to allocate them in a structured manner. For routers and routing protocols to operate efficiently with minimal overhead they perform a feature called summarization [34]. This is the ability to advertise a block of addresses rather than every single address. If the allocation of IP addresses across the network is not well structured, address summarization may not be possible.

In a large network, static configuration of every router would be unmanageable. IP routing protocols like RIP, EIGRP, OSPF, BGP, etc., enable routing updates between routers. OSPF and IS-IS are hierarchical routing protocols based on areas within the same autonomous system (AS), lending well to scaling [34]. The purpose of these is to divide the AS into limited size groupings so the amount of routing information is within the capability of the links to support the traffic and within the processing power of the router's CPU and memory. OSPF has algorithms to perform load sharing on alternate paths. OSPF makes use of the shortest path first, or Dijkstra algorithm to compute the shortest path to each network [35].

BGP can dynamically determine route availability for very large networks and has become the standard for Internet routing and MPLS routing between customer edge and provider edge routers. BGP was designed to exchange routing information between very large ASs and has provided stable Internet routing for decades. It can be set to abide by policies directed by commercial considerations specifying which carrier network to offer routes given sets of customer networks [34]. BGP4 is the most widely adopted inter-domain routing protocol with four basic components, speaker, peer, link, and border router [55]. A speaker is a host or router that executes the protocols. A peer is when two BGP routers form a connection in a BGP session, being either internal or external depending on whether in the same or different AS. A link is the internal or external connection between peers. A border router is an interface to a physical network shared with routers in another AS.

An issue with BGP in an IPv4 environment is the lack of strong source authentication. There are three options to address this vulnerability, IPSEC, TCP/MD5, and BGP MD5 [57] – [59]. The IETF introduced IP security architecture (IPSEC) to protect the confidentiality of BGP control traffic and the integrity of the TCP connection between BGP speakers. The encapsulating security payload is used to provide data and partial sequence integrity and peer authentication. The TCP message digest algorithm comes from RFC2385 and is widely deployed, but its strength is suspect. There is also a BGP message digest algorithm for peer authentication, but it does not protect against TCP reset attacks. Another suggestion is peer-to-peer encryption, where all BGP messages between peers use session keys exchanged at BGP link establishment time [55]. This provides integrity and authenticity of all path attributes whose values are valid for one AS hop and can be implemented between all BGP peers.

To deal with routing in large networks the routers must be dimensioned accordingly. Tests carried out on modelled customer networks have shown estimation of CPU power and memory size a non-trivial exercise [36]. General design rules are subject to strong caveats, and medium to large scale designs must be assessed on an individual basis making sure router memory size is dimensioned correctly. Some routers need to hold databases and tables for many ASs and must be equipped with adequate capacity to store this information on top of normal buffering, state information, housekeeping, policies, and security.

One of the challenges in routing is security. The distinct threat consequences against routers include disclosure, deception, disruption, and usurpation [54]. Disclosure is an event in which a router successfully gains unauthorized routing information. Deception is an event that results in a legitimate router receiving false data and trusting it. Disruption is an event that causes the function of legitimate routers to be interrupted or prevented. Usurpation is an event where an attacker acquires control over an authorized router's system services or functions. The damage resulting from these threats can be congestion, delay, looping, instability, and overload [55]. Vulnerabilities and threats can be minimized or eliminated by adopting the following security services [56].

Table 1 Security Services

Service	**Definition**
Confidentiality	Protecting data from being disclosed to unauthorized entities or processes
Integrity	Protecting data from being modified or destroyed in an unauthorized way
Authenticity	The verification of the identity claimed by a system entity
Access Control	The protection against unauthorized use of system resources
Non-repudiation	The protection against false denial of communication services
Availability	The assurance that an authorized entity can use resources when necessary
Timeliness	The assurance that a router uses the latest routing messages to make routing decisions

Design faults and configuration errors account for a substantial number of network problems and are exploited by over 65% of attacks [67] [69]. Most of the attacks on the network infrastructure begin with spoofing the IP source address of the victim. This can be mitigated with network partitioning [68]. A network partition is safe if two hosts that should not communicate according to network security policies, do not belong to the same broadcast domain or zone. The flow between them to be blocked should cross a filtering component like a firewall. The more troublesome attacks for the Internet are DDOS attacks which employ forged source addresses. Ingress traffic filtering can be used to prevent DDOS attacks propagated from behind an Internet service provider's aggregation point.

Another challenge in routing is convergence time. Reducing the time taken for all routing tables to become stable after a state change is one of the key factors in maintaining the availability of a network. Large networks with a poor convergence time will result in connection failures or delays that will potentially affect a large part of the user population. Convergence is enhanced by use of an area hierarchy, address summarization at boundaries, transmitting only routing changes, and sending triggered updates [34].

Users increasingly want to distinguish IP traffic flows across a network which in turn necessitates the classification of different traffic types, applying ingress policing, traffic shaping, and priority queuing. [41] defines common application flow measures and targets existing for MNCs in the following table.

Table 2 Application Flows

Application Flow Measures and Targets						
Application	Type	Target Bandwidth (Kbit/s)	Target Loss (%)	Maximum Delay (ms)	Effective Priority (10 = high)	Quality (red/amber/green)
VoIP	Real time	32	0	150	10	Special MOS (mean opinion score)
SAP	Transaction	50	2	150	8	Amber = delay between 100 & 150, red = delay over 150
Oracle	Transaction	20	3	200	8	AFM (adobe font metrics)
Video	Real time	1500	1	200	8	Special MOS
Internet	Background	30	3	500	4	Amber = bandwidth

						between 25 & 30, red = bandwidth < 20
Email	Data	25	5	n/a	3	Av. Over 1 min, av. Over 10 min
FTP	Background	25	5	n/a	2	Amber = bandwidth between 20 & 25, red = bandwidth < 20

From the table, voice is the most critical application for MNCs. Delays greater than 30 ms can make echoes intolerable for voice, but if echoes are suppressed, delays of 150 ms are acceptable [46]. Delay requirements have to be fulfilled at both endpoints of a VoIP call and can be guaranteed by a VPN, so latency limits are satisfied in the transport network. To avoid echoes, international delay standards for the telephony network require a maximum cross-exchange delay of 450 μs and a maximum national delay of 24 ms [46].

Assuming a large VoIP network with a huge number of customers, it is necessary to take quality of service as well as economic criteria into account during the design phase. The VoIP network is divided into two logical components, pure IP based service in the access network and QoS guaranteed in the transport network [94]. The access network includes the VoIP nodes, while the transport network serves the purpose of carrying the aggregated VoIP traffic between the various access areas. The main parts of the transport network are the edge routers, the transit routers, and the connections between them. During VoIP network design, the traffic distribution between the VPN nodes cannot be considered a fixed input since it largely depends on the gateway assignments. The traffic of any given VoIP node x is modeled by a bandwidth demand value tr_x, that shows the amount of capacity needed to satisfy the calls generated and received by the VoIP users in the given node [94].

Voice is critical for business. Therefore, in the case of a VPN element failure, the traffic handled by the corresponding router or link can be redirected onto backup paths unaffected by the failure. In case the failed element is an edge router, the served VoIP endpoints are reassigned to their respective backup gateways. It is important in the transport network for only one element at a time to fail, so a shared backup path protection scheme can be easily applied [95] [96].

The differentiated services (Diffserv) model for applying quality of service is the standard for existing MPLS networks from all service providers [34]. The Diffserv model of the IETF relies on setting precedence bits in the header of the IP packet. The expedited forwarding (EF) class supports low latency and jitter for voice-over-IP. The assured forwarding (AF) classes give a next grade of priority to other mission critical applications. The default class is reserved for non-critical traffic and bursting schemes can be configured between classes [42]. Routers and LAN switches can set these precedence bits in a predefined policy or act on them in the event of congestion. The LAN switch is an ideal place to set precedence since routers often run security policy and other resource intensive functions. We must be careful configuring LAN switches to avoid security issues like VLAN hopping that exploit configurations to allow communications between different VLANs [66] [69]. In addition to IP layer precedence, Ethernet precedence has also been defined using the IEEE 802.1p standard. Diffserv is typically a feature of MPLS networks and could be a possible issue with cloud services on Internet connectivity.

C. Software Defined Networking Concepts

Routing environments are being supplanted by new technologies. The new paradigm in enterprises today is the advent of software defined networks (SDN) [15]. With SDN, the network virtualization empowers enterprises to exploit virtual local, storage and WANs to meet the growing needs with reduced capital expenditures and operating expenditures. The virtual servers, storage, and network components need physical pools of compute, memory, disk, and network resources requiring proper design and plan to enable SDN. With SD-WAN network operators can combine multiple site-to-site links into a single logical network circuit managed by a single, centralized SDN controller [65]. The SDN controller manages the links under its control and intelligently routes data over them based on QoS rules set by network operators. SDN controllers also provide real time monitoring, which allow them to take link conditions (latency and packet loss) into account when routing packets from one site to another. Most network traffic is routed through the SD-WAN tunnels and the ISP is reduced to being a bandwidth provider. Switching ISPs is as simple as rerouting the tunnel over the new ISP connection.

SDN is a technique for building a programmable network by controlling switches and routers in the network via software [81]. Routers or switches are managed by a named SDN controller that belongs to the data plane. The data plane forwards traffic according to the decision made by the control plane. The control plane determines the network traffic destination. SDN architectures have two application programming interfaces (APIs) [81]. The API of the control plane is called the northbound API, and the API of the data plane is called the southbound API. SDN is used to create a network slice. A slice is a virtual network operated and managed by SDN. By dividing the physical network, it is possible to construct a virtual network for each user or application as a virtual private network or virtual local area network. There is no limit to the number of slices as long as the physical network has bandwidth available. Network slicing is supported on 5G NR, so it is possible to give a user or application secure, reliable connections throughout the network [11]. However, SDN does have problems like scalability. If more than one SDN controller exists in the network, the switches and routers will receive instructions from multiple controllers. This could cause disruption in the network [82] [83].

Network orchestration refers to arranging and organizing network service units to balance the various components of the network and generate the service which can meet the requirements of users [38]. Orchestration is based on building the virtual network in the infrastructure environment provided by the cloud system to carry the upper layer service. SDN implements the flexible control of network traffic by separating the network equipment control plane and data plane making the network pipeline more intelligent [39] [40].

Some SD-WAN appliances have WAN optimization as a part of their feature set. An enterprise with several branch offices might have a series of smaller WAN optimizers at each branch, with a much larger capacity optimizer handling all branch requests at the main campus DC. Located at these two points, WAN optimizers work in tandem to reduce traffic load across the WAN. The compression ratio depends on the type of data transmitted [102]. ASCII text is highly compressible, whereas Secure Sockets Layer encrypted traffic is less compressible. Most vendors use compression algorithms based on the popular Lempel-Ziv-Welch compression scheme. If the traffic is heterogeneous, a specific algorithm might not be beneficial. In this case, the compression dictionary’s performance and size are the most relevant considerations. The larger the dictionary, the more patterns it can store and thus index for reduced WAN transmission. Dictionary size reflects the relevant storage allocated to it, whether memory or hard drive.

Another simple practice to limit WAN traffic is to use a cache to store frequently accessed data at the branch site [102]. Then, when a branch worker requests this information, he or she can retrieve it locally via the cache as opposed to requiring access to the campus DC. The WAN optimizer that controls the cache partially acts as a filesystem application proxy. Such proxy behavior can be extended even further with the addition of more application awareness to the network device. An application specific proxy can understand protocol messaging and actually answer client requests to prevent additional WAN queries. With cloud services, SD-WAN with optimization can be setup in a VM inside the cloud service provider's architecture.

With SDN comes opportunities for energy efficiency in network design. The authors in [43] estimate the power consumption of the Internet to be about 0.4% of the total electricity consumption in broadband enabled countries with access rate of 1 Mbps. As access rates increase between 100 and 1000 Mbps, this percentage will dramatically rise to over 10% of total electricity consumption. The idea is proposed to divide a day into several time slots, during which traffic loads have similar statistical behaviors [44]. At the beginning of each time slot, virtual topologies with SDN reconfigure to allocate just enough network resources for traffic loads to reduce energy consumption caused by over provisioning. Compared with static energy efficient design, dynamic design through SDN can obtain about 30% less energy consumption [44]. This can also be achieved in Ethernet utilizing the IEEE Energy Efficient Ethernet standard [45]. This technique changes link speed according to the data traffic demand. Other techniques to consider are employing low power voltage LSI to reduce power consumption, using dc power supplies to reduce conversion loss, and using functions virtualization for virtual routers [45].

D. Issues and Challenges in Networking

One of the issues to understand in enterprise environments is how to handle link loss on large networks. The existing loss rate inference methods in large scale networks are rank based, experimental design based, and matrix decomposition based [16]. Rank based methods have a high degree of accuracy, but the number of paths needed to detect equal the rank of routing matrix and is a very large number, so the probing overhead is too large [17][18]. Matrix decomposition-based methods need to detect a relatively small number of paths, but the downside is high error rate [19][20]. Experimental design-based methods have a smaller path to detect with higher accuracy than matrix decomposition, but the calculation process is time consuming. Bayesian experimental design path selection is the optimal method for link loss inference [16]. The goal of the Bayes design is to maximize the expected utility of certain test results. The utility is usually provided as a metric which can be accurately measured indicating a good experimental design should ensure the optimum decision is maximized. The Bayes approach strikes a balance between the overhead and accuracy of detection in large-scale networks.

One of the challenges in enterprise networks is the development of mobile applications with issues ranging from the need of implementation of services to integration with web and cloud-based applications [21]. While these services are well understood and developed for web-based applications, they are still challenging for mobile applications. Integration issues are also challenging in developing mobile cloud applications preventing application effectiveness [22]. Four of the areas of focus for mobility applications are collaboration, sharing, awareness, and operational interoperability [23].

The primary requirement of teamwork applications is to support collaboration among members of a team. The teamwork establishes a goal, and based on that goal, a collaboration strategy is followed (synchronous, asynchronous, or both). To ensure basic operation of a team, it is fundamental to share information among its members. This information usually includes documents, files, workplan, messages, discussions, contact lists, and collaboration agendas. For sharing dynamic information, it is necessary to implement synchronization mechanisms and notification services for conflict resolution [24]. Members of a team need to be informed on the action carried out by other team members and react accordingly. Awareness can take various forms such as availability awareness, context awareness, process awareness, etc. Mobile applications should also support operational and technological interoperability. Members of teams should be able to operate under different platforms, devices, and networks.

With mobile applications, synchronization and notification are two of the challenging issues [23]. The information sharing, awareness, task states, etc. must be kept synchronized at both server and mobile devices. While easier to synchronize at the web application server, it is more challenging to ensure synchronization when mobile users are allowed to make local changes at their devices and propagate changes to all members of the team. Data synchronization aims to ensure the same data in two or more different locations. We want the data to be the same at different mobile devices when a user makes a change reflecting on all devices. Notification of events can be implemented either in pull or push modes. In push mode, events are automatically reported to the recipients, while in pull mode, recipients decide when to receive notifications. An open-source library developed in Java by Apache enables software developers to select the output and the level of granularity of messages at runtime rather than compile time [23].

Mobility also has the issue of dealing with opportunistic networks regarded as wireless ad hoc networks that are delay tolerant. An example would be the millions of IoT devices that have become a part of the Internet via mobile providers. Several flood-based routing protocols have been proposed with UDP as the transport protocol to handle these delay tolerant networks [90] [91]. Epidemic Routing is an approach proposed by Vahdat and Becker to distribute application messages to hosts within connected portions of ad hoc networks [92]. In this routing protocol, two nodes exchange their messages when they are within communication range, so the message will eventually be copied to the destination node.

Epidemic Routing (EPI) protocol works by each host maintaining a buffer consisting of its originated messages as well as messages of other hosts buffering in it. A hash table indexes this list of messages, keyed by a unique identifier associated with each message. Each host stores a bit vector that is a compact representation of all the messages being buffered at the host. When two hosts come in communication range of each other, the host with the smaller identifier initiates a session with the host with the larger identifier. During the session, the two hosts exchange their summary vectors to determine which messages stored remotely have not been seen by the local host. In turn, each host then requests copies of messages that it has not yet seen.

EPI makes message transmission in the network similar to viral transmission. Under ideal conditions, such as unlimited bandwidth, buffer and energy, EPI can perform well [93]. However, its performance is poor when TCP is implemented in opportunistic delay tolerant networks. Because of the mobility of nodes, opportunistic networks may cause link failure which leads to intermittent connectivity, which can degrade the network performance. Because EPI is a multipath routing scheme, there are possibly many copies of the same packets in the network which results in receiving multiple copies at the destination. In order to improve the performance by deleting this kind of redundant multicopy data packets, a cross-layer design based on TCP and EPI named ACK-EPI can be implemented [89]. ACK-EPI can avoid the packets that have already been delivered being forwarded again in the network.

Another challenge for network design is node placement. Well known graph centrality metrics are used to measure the importance of a node in terms of betweenness, closeness, and degree [25]. Betweenness is defined as the number of the shortest paths that flow through a node signifying a node's importance in communication [28]. Closeness is the inverse of the sum of the shortest paths from a node to every other node indicating efficiency of a message's diffusion in a network. Degree centrality is the number of links incident to a node and can be viewed as the importance of connectivity of a node. The reason these centrality metrics are chosen is twofold. First, an adversary with knowledge of the network topology can attack the most central nodes with the intention to cause the most damage [26]. Second, from a load-balancing perspective, the flows are more evenly distributed in centrality-balanced nodes. Therefore, centrality metrics provide a good means of measuring resilience and load-balancing traffic [27]. While degree centrality provides local information about a node's significance, the betweenness and closeness centrality metrics provide global information about a node's significance. The average nodal degree x is obtained by multiplying the number of links by two and dividing it by the number of nodes in a given network topology [85]. Simulation results in studies have concentrated on showing how the working and spare capacity requirements of each network type vary with the network average nodal degree. Liu, et al. argue this metric is only a coarse indicator of how sparse or dense a given topology is [85]. It carries insufficient information on network topology structure and using the average nodal degree for describing connectivity may lead to misleading findings. Algebraic connectivity is a more informative metric. Algebraic connectivity is defined as the 2nd smallest eigenvalue of a Laplacian matrix of a topology and is a more sensitive measure of connectivity [86] [87]. It is proposed to quantify the importance of a node, or a link based on the algebraic connectivity of the network's graph, because the larger the algebraic connectivity, the more connected the graph will be [85]. The nodes or links that cause more server reduction in the algebraic network connectivity has higher importance and should need more protection. In addition, both working and spare capacity allocations could benefit from adding critical nodes and links to maximize the algebraic connectivity of existing networks.

It is observed that closeness improvement methods always yield the highest number of added links, which implies that it tends to select shorter paths [29]. On the other hand, both betweenness and degree improvement yield a fewer number of links. The degree-based improvement method yields the lowest number of links added with small differences with respect to betweenness-based improvement. It is observed that even though the closeness-based improvement consistently yields the highest number of added links, it fails to provide better flow robustness values than both betweenness and degree improvement methods in most attacks [29]. This implies that having a larger number of links in each node does not necessarily guarantee better resilience. Moreover, adding links without a careful improvement of networks may not yield any gain in terms of resilience and performance. Overall, results show the degree improved nodes outperform the other two improvement methods [29].

E. Resiliency, Survivability, and Availability

Improvement methods are all about resiliency. When addressing resiliency, the high availability seamless redundancy (HSR) introduced by IEC 62439-3 is drawing much attention because of its capability of providing high availability with a zero-failover time [30]. Unlike its counterparts, HSR uses a broadcast and duplicate filtering forwarding rule through which loop-free simultaneous transmission over multiple paths becomes possible [31]. In addition, being applicable to any topology, the HSR scheme offers a large degree of freedom to the network designer. However, designing HSR topologies is a nontrivial task, especially for the case of highly connected mesh networks in which full utilization of their inherent redundancies may produce availability much higher than demanded [32]. *Therefore, a significant reduction of deployment cost can be achieved by means of efficient design.*

The IEC 62439-3 recommendation introduces two Ethernet based redundancy methods sharing the capability of zero failover time, the parallel redundancy protocol (PRP) and the HSR [30]. However, the use of PRP necessitates a full duplication of network physical topology and thus it is very costly [33]. HSR alleviates this requirement while retaining other favorable properties of PRP [31]. The basic principle of HSR is to duplicate frames and simultaneously transmit them over disjoint paths. HSR networks are restricted to HSR-capable nodes having two or more Ethernet transceiver ports sharing the same MAC address and represented to the upper layers as a single Ethernet interface through an additional communication layer called the link redundancy entity (LRE) [31].

To avoid loops in HSR, a duplicate discard mechanism is implemented at the LRE of a participating node. When a HSR node sends a frame generated at its upper layer, the frame will be duplicated at the LRE and each of the duplicates will get a HSR tag before being transmitted over each port. A receiving node forwards the frame to others, except when it has already sent the same frame in the same direction, based on the combination of the sequence number and source MAC address. A destination node receives duplicates of a frame from different ports and passes the first frame to the upper layers discarding other duplicates [31].

Along the same lines of resiliency is survivability. Network survivability is defined as the ability of a network to maintain its communication capabilities in the face of equipment failure [61] – [63]. It can take the form of adding spare capacity throughout the network, so traffic affected by a failure could be re-routed on this spare capacity to the destination. One of the significant components of survivable network design has been the efficient allocation of spare capacity throughout the network. Spare capacity can more than double the capacity costs and add significant overhead [37]. When designing a scheme to allocate spare capacity there are several trade-offs made. These trade-offs are regarding redundancy, complexity, and timing [37]. Redundancy is the amount of spare capacity compared to the minimum working capacity. Complexity is the amount of coordination required to commission and decommission restoration routes. Timing is the required time to commission and decommission restoration routes.

One approach for survivability is to enforce path diversity at the time of flow allocation [103]. This way, demand volume can be split into more than one path. A restriction can be put on the amount of flow on each path by introducing diversity constraints [104]. In case of a single link failure, only the demand carried on one of the paths is lost, while the rest of the demand is still carried in the network providing partial survivability. Another approach is to provide network survivability by maintaining a pair of disjoint paths for each service class between source and destination. In the event of link failure, flow on the affected path can be switched to the alternate path. This is known as MPLS Fast Reroute [105] [106].

An approach to incorporating survivability into individual paths, rather than identifying alternate configurations to be used in the event of failure, is through MPLS Fast Reroute [107]. One consideration for this is end-to-end fast reroute. In this case, each traffic flow has a readily available end-to-end alternate path that may be used to route the demand on a hot standby basis in case of any single link failure. It is assumed the network is dual connected, and to make each of those routes survivable, a diverse route is guaranteed available for every customer demand.

A different approach to designing survivability into the network is to selectively decide those customer demands that would be directly impacted by a failure [107]. This has the advantage of allowing faster computational time since each sequential failure state needs to consider fewer traffic loads than those considered in the initial design. From a realistic network perspective, it does not disturb flows not affected by the failure. The disadvantage of this approach is it typically could lead to a higher cost network because the design allows fewer elements to be adjusted to minimize cost. As networks get larger, the relative cost of making the network survivable goes down. As a network of a given number of nodes increases its connectivity, the cost of survivability tends to go down. However, these patterns do not always hold true depending on the actual network topology, connectivity, and demand volume [107].

Demand-wise shared protection (DSP) was developed to resemble the simplicity of 1+1 automatic protection switching (APS), while capturing some of the efficiency of more complex survivability schemes, like shared backup path protection (SBPP) or span protection [37]. DSP shares spare capacity by splitting up working capacity for each demand pair. This traffic is split into multiple disjoint routes. If n units of capacity are routed on k disjoint paths, the spare capacity required to provide full single failure restorability is n/k + 1. There is a trade-off between the increasing length of the working paths required to add disjoint paths and the reduction in spare capacity.

There is a probability that two or more failures could occur simultaneously and to achieve a greater degree of availability, the survivability schemes must adapt to handle multiple failures. The network must be at least tri-connected to achieve full dual failure restorability. There are three dimensions to the definition of dual-failure restorability, network, failure, and impact [37]. The network scope deals with whether restorability is measured as a network average or defined at the demand level. Failures may or may not impact a given demand, so there are dual-failure scenarios not used in the calculation. The last dimension is whether dual-failure restorability is an average for a network or a minimum for any failure scenario.

When DSP utilizes multiple paths to reduce redundancy, there is a given level of dual-failure restorability [37]. This efficiency was fully utilized for networks with lower implementation factors. As the implementation factor of the network increased there was a strong linear component to the total cost. The capacity cost continues to rise for the DSP networks as the implementation cost is increased. The average nodal degree was still reducible due to having single failure restorability requirements. The significance of this is the required extra path for dual-failure restorability increased the exposure to failures more than it protected capacity in the network. Increasing dual failure restorability to levels between 50% and 70% had negative effects on the overall network availability [37]. Routing on multiple paths increases exposure to failure not counterbalanced by spare capacity on the other spans. As a result, some levels of dual-failure restorability had a negative impact on availability.

Availability can be expressed as the probability that a system will be found in an operational state at a random time in the future [60]. The availability of an element x is thus defined by

$$A_x = \frac{MTTF_x}{MTTF_x + MTTR_x} = \frac{MTTF_x}{MTBF_x}$$

with MTTF and MTTR representing the mean time to failure and repair, respectively. MTBF represents the mean time between failures. Similarly, network availability can be represented by the ratio of the time that the network is operational in a given period and can be evaluated by considering the availabilities of all the elements in a network.

The probability of network failures varies depending on the interconnect hardware and software, system size, usage of the system, and age [47]. Stochastically speaking, all possible failure modes are not possible. They will be bounded by probability, geographic events, or other network characteristics [70]. A mission critical network is typically considered functional with a smaller set of its services in an emergency situation, discarding less important traffic temporarily. Mission critical networks typically do not have highly connected uniform topologies [70]. It is more likely they are sparsely connected groups of highly connected nodes. Network failures constitute between 2% - 10% for the high-performance computing systems at Los Alamos National Laboratory, over 20% for LANs of Windows based servers, and up to 40% for Internet services [47] – [49]. Wilson showed a constant failure rate of approximately seven unstable links between switches per month and a total of approximately thirty disabled network interface controllers over an 18-month period for an IBM Blue Gene/P system [50].

It is important to understand the possible network states when considering failures. If the components have equal probability of failure, ordering the states by most probable to least probable is equivalent to starting from left and working to the right as network states grow [70]. The different states can be represented by

$$Network\ States = \binom{N}{k} = \frac{N!}{k!\,(N-k)!}$$

In this study’s algorithm, the network space classification is defined as a representation of all network states as non-feasible, success, and failed [70]. A failed network state causes the network measure for the network at that state to be less than a preset threshold that defines minimum network function.

F. Capacity Planning

Availability, survivability, and network states lead to a discussion about growth and capacity planning. Strategic capacity planning is designed to assist network planners in assessing the impact of a bulk forecast demand on the transport network in terms of bandwidth and equipment required to support the demand [84]. It does not model the network down to the detail level, but it does model the network enough to determine when capacity on key elements will be exhausted. Capacity planning should identify where bottlenecks are, incremental capacity requirements, where additional switches are needed, and where routing efficiency is needed. The traffic forecast should be broken down into a number of product lines and details of the load on each network element by product type should be given [84]. The view of network load by product type is important as network planners are often interested in knowing which product is driving capacity to exhaustion in certain parts of the network. An important requirement of the capacity planning model is details of in-station connectivity. In large transport networks with multiple switches in the same locality, the in-station connect is a key element in planning and dimensioning the network. It is not possible to plan in-station connectivity in isolation from the rest of the network as the connectivity will be determined to a large extent by the traffic flows from the external connections through the building.

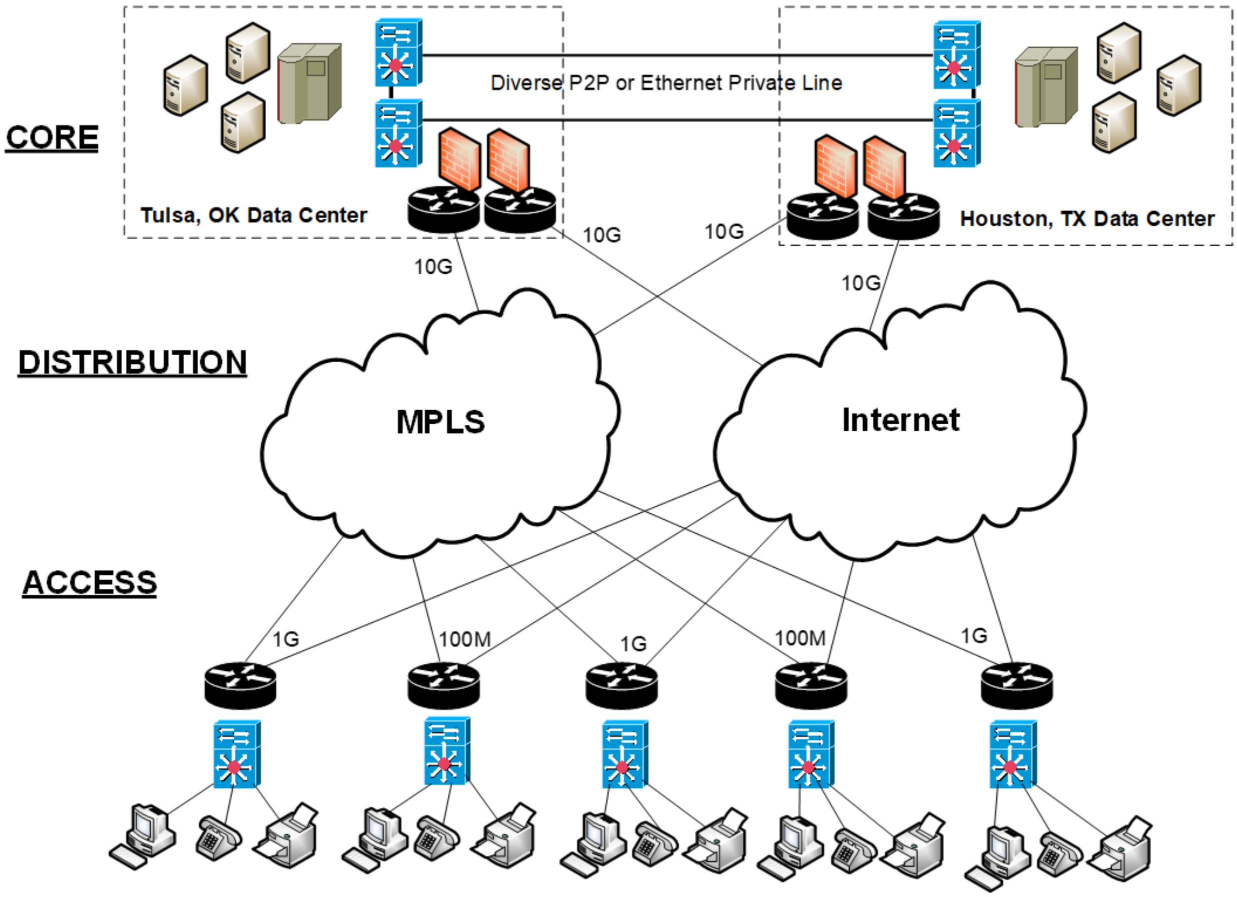
Capacity planning tools are only as good as the information provided to them. Generating an accurate traffic forecast for forward capacity planning must be an overriding consideration [84]. There is likely to be a wide range of routing strategies and specific problems to investigate with respect to achieving a minimum cost network. It makes sense to build a routing engine that is generic and can be tailored to a particular problem without large overhead in development costs. Routing rules can be applied to least hop, least distance configurations, or some other cost metric. Various metrics can be defined to try alternative routing strategies and analyze the effect of this on the network and associated costs. The capacity planning routing engine can be used to investigate an alternative set of rules to improve the overall routing efficiency within core transmission networks [84].

Considering all the information presented in the literature, this thesis has a unique approach for network design as it relates to cloud migration. Network models, service infrastructure, routing, security, mobility, survivability, availability, etc., prove the network design and engineering problem is NP-hard and very challenging to account for all variables in a single algorithm. However, as companies migrate from private networks with private DCs to the cloud, we have historical data to analyze, which will provide a baseline for building a cloud solution based on Internet connectivity.

III. Methodology

Twenty-five Fortune 500 companies were chosen from different industries to get a good sample across different business environments. The twenty-five companies selected for analysis include some of the largest MNCs in banking and finance, retail, oil and gas, home building, insurance, and consumer services. All companies have private MPLS networks with DC centric environments with both time-division multiplexed (TDM) and Ethernet access circuits connected to their respective MPLS VPNs at each of their locations. Each organization has a similar architecture comprised of core, distribution, and access with redundant DCs typically located in each region around the world. A typical network diagram showing the basic topology is below.

Figure 1 Typical Network Diagram



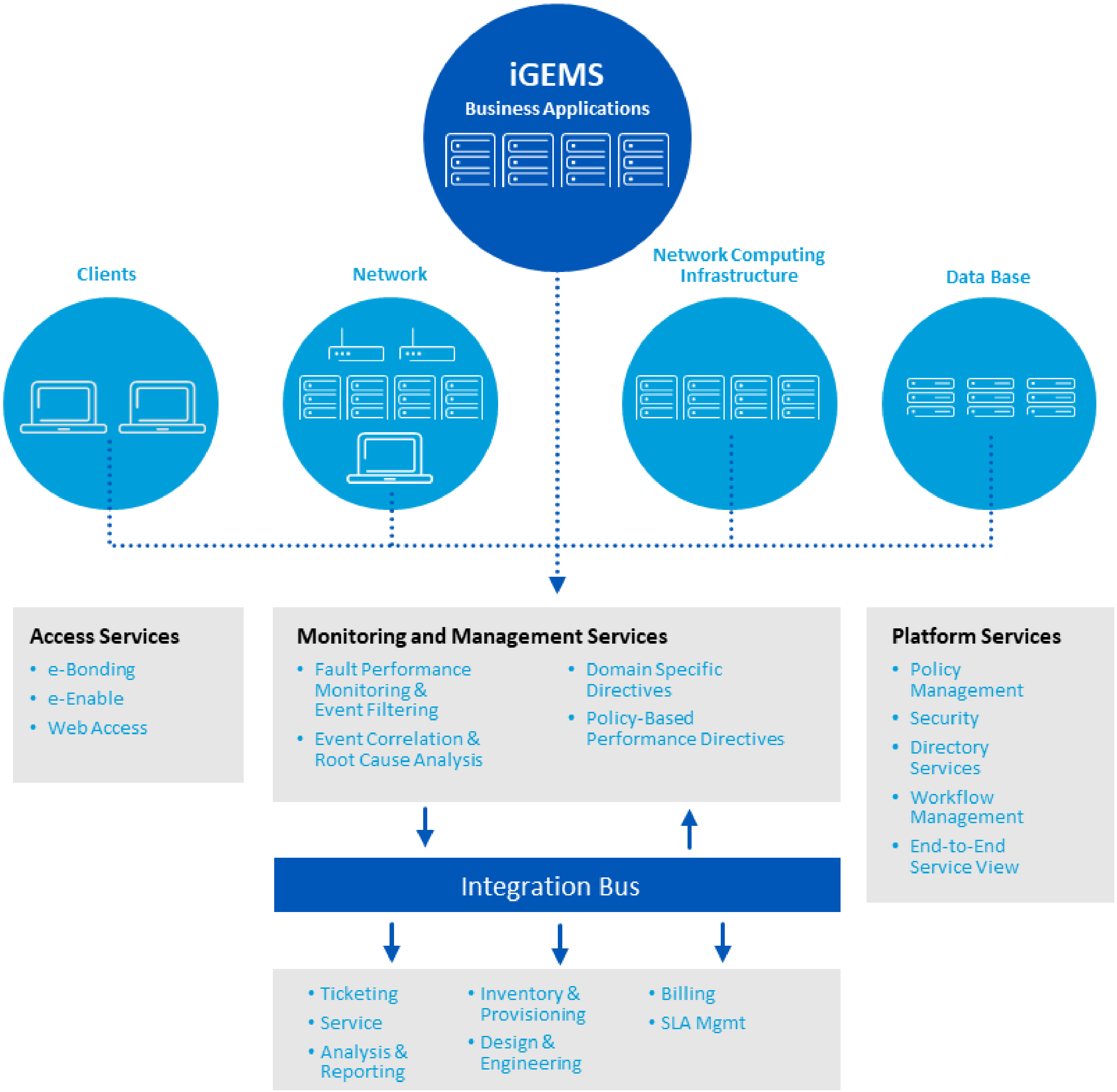
All companies analyzed had class of service (COS) configured on their MPLS circuits for critical latency sensitive applications like IP voice and IP video. Many of the circuits analyzed for each of the companies were part of diverse pairs providing diverse paths, central offices (COs), points-of-presence (POPs), and customer premise equipment. The circuits had bi-directional forwarding detection (BFD) configured at layer 2 of the protocol stack to detect any anomalies between the customer edge routers and the provider edge routers. At layer 3, routing protocols like border gateway protocol (BGP) were configured for diversity to primary and backup data centers. The circuits are different sizes ranging from 1.544 Mbps T1 to 10 Gbps Ethernet depending on the perceived bandwidth requirements at each site. A total of 29,675 circuits across the twenty-five companies were examined for a 12-month period from August of

2020 to July of 2021. Utilization data was gathered from each of the circuits for inbound and outbound utilization on 15-minute intervals throughout each day for the entire 12-month period.

The network management system (NMS) used to gather the data is a combination of off the shelf products and custom development creating an integrated global enterprise management system (iGEMS) platform. The management model is follow-the-sun, so network operation centers (NOCs) existing around the world handoff to each other as the workday ends. The network is being monitored and data is collected 24 hours per day, 7 days per week, 365 days per year (24x7x365). It is difficult to find a single application to perform all the functions necessary for comprehensive management to meet the ISO FCAPS (fault, configuration, accounting, performance, security) model, so an integrated platform approach was taken for this study.

iGEMS uses several tools based on simple network management protocol (SNMPv3), remote monitoring (RMON2), and proprietary protocols like NetFlow from Cisco Systems and J-Flow from Juniper Networks. SNMPv3 is the latest SNMP version to become a full standard. Its introduction has moved SNMPv1 and SNMPv2 to historic status. SNMPv3, which is described in RFCs 3410 through 3415, adds methods to ensure the secure transmission of critical data to and from managed devices [71]. RMON2 allows the collection of statistics beyond a specific segment's MAC layer and provides an end-to-end view of network conversations per protocol. The network manager can view conversations at the network and application layers. Therefore, traffic generated by a specific host or even a specific application on that host can be observed [71]. These tools were used to gather the inbound and outbound data for all the circuits examined in the 12-month period. A software architecture diagram for iGEMS with modules and associated services is located below.

Figure 2 iGEMS Architecture



A critical part of iGEMS is the EMC SMARTS Network Configuration Manager (NCM). NCM is an automated compliance, change and configuration management solution that delivers industry-recognized best practices [109]. In addition, it is a collaborative network infrastructure design tool that controls change processes, provides network device and service configuration transparency, and ensures compliance with corporate and regulatory requirements, to enable us to ensure the security, availability, and operational efficiency of the network. NCM is an automated support tool for all facets of the network infrastructure lifecycle, seamlessly integrating critical design, change, and compliance management requirements.

The iGEMS platform includes a distributed IBM DB2 database for warehousing all the data gathered from the network. The database is sized to handle up to two years of active data for historical analysis, root-cause analysis, performance management, and capacity planning. After two years, the data is archived and stored securely for historical analysis if needed. The reporting engine for iGEMS is provided by Infovista, offering custom reports on the data collected by the NMS. Data is available for hourly, daily, weekly, and monthly reports for COS, performance, and topology. The reporting engine has exporting capabilities for different file formats including text, MS Excel, Adobe PDF, and XML. The text and Excel formats would allow importing into different tools for analysis. The PDF format is static content used for reporting purposes only. The XML format is used heavily in front-end and back-end web development with industry standard APIs using it to transfer data. XML is also used in mobile application development for the Android operating system, so this format allows customers to use the data in their own management tools.

Monthly inbound and outbound utilization reports were produced for each company’s circuits with ingress utilization BusyHr%, ingress utilization Peak%, egress utilization BusyHr%, and egress utilization Peak%. An example of the raw data collected for each company on a monthly basis is located in Appendix A. This raw data is for the smallest network in the samples. Some of the companies in this study had networks with thousands of circuits. BusyHr% is the busy hour value of measurement over the selected time frame for a particular circuit. Peak% is the largest utilization measure made over the selected time for a particular circuit. BusyHr% is critical in the analysis because this is the time period when the circuits have the most sustained traffic. The busy hour data was used to calculate the mean and standard deviation for monthly and yearly analysis for each circuit. The monthly averages calculated at busy hour for each company are below.

Table 3 Monthly Averages

Company 1		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	8.50	13.78
November	8.64	11.08
December	7.38	9.40
January	7.28	9.51
February	7.66	10.40
March	9.26	12.34
April	8.63	9.69
May	9.81	10.20
June	8.36	10.14
July	7.90	9.02
August	9.12	10.73
September	8.75	10.50

Company 2		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	4.82	4.7
November	14.56	13.65
December	12.55	20.25
January	15.85	22.04
February	17.55	20.41
March	18.73	28.36
April	18.55	28.32
May	20.40	28.53
June	21.05	27.70
July	18.22	27.50
August	16.23	26.47
September	18.50	27.33

Company 3		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	45.13	62.46
November	43.85	60.69
December	40.20	55.79
January	45.96	62.88

February	44.81	63.96
March	45.29	71.41
April	53.01	74.08
May	45.80	62.50
June	52.23	74.34
July	46.53	69.63
August	50.94	69.65
September	52.14	62.51

Company 4		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	22.06	34.42
November	23.19	30.25
December	23.63	34.99
January	25.78	50.25
February	25.07	37.06
March	25.72	46.87
April	23.72	38.98
May	24.55	38.81
June	24.05	37.14
July	21.05	30.11
August	21.99	49.99
September	23.22	39.25

Company 5		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	15.18	16.45
November	12.68	15.04
December	12.32	14.61
January	12.80	14.30
February	11.71	13.40
March	11.82	13.76
April	11.57	19.73
May	9.94	15.28
June	10.69	15.51
July	11.07	14.08
August	9.89	17.00
September	10.50	16.51

Company 6		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	53.21	66.67
November	54.48	46.32
December	57.30	55.00
January	49.25	44.16

February	55.97	44.40
March	53.48	51.87
April	59.45	66.41
May	62.40	49.90
June	58.17	46.23
July	48.64	47.16
August	48.71	44.57
September	51.50	47.25

Company 7		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	9.99	9.38
November	12.03	7.41
December	11.72	9.03
January	12.57	9.57
February	10.52	6.81
March	11.24	8.39
April	9.31	6.30
May	6.33	6.53
June	5.50	4.62
July	6.79	6.25
August	6.73	5.26
September	6.70	6.33

Company 8		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	11.61	23.44
November	12.78	30.36
December	13.46	25.55
January	14.30	29.79
February	15.45	28.90
March	14.85	24.92
April	14.15	21.04
May	14.58	34.17
June	14.17	30.94
July	13.16	33.04
August	14.99	32.70
September	14.50	32.50

Company 9		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	37.66	43.27
November	36.29	53.81
December	38.08	51.33
January	35.71	48.78

February	38.84	53.54
March	38.50	48.53
April	38.53	49.01
May	40.14	54.23
June	39.12	50.13
July	37.09	47.53
August	37.77	49.41
September	38.12	50.11

Company 10		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	17.02	51.71
November	14.33	43.76
December	15.92	46.03
January	15.97	46.02
February	17.06	48.38
March	17.73	48.84
April	16.37	51.40
May	18.00	48.72
June	17.89	52.21
July	16.11	48.88
August	17.22	46.36
September	17.25	48.50

Company 11		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	20.51	36.96
November	22.86	40.89
December	21.15	39.87
January	21.33	34.61
February	24.63	36.49
March	20.13	35.67
April	25.00	38.35
May	21.68	26.17
June	21.09	28.56
July	29.00	31.44
August	28.00	28.83
September	28.50	30.11

Company 12		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	0.87	2.43
November	0.83	2.53
December	0.83	1.43
January	0.78	1.19

February	0.76	1.18
March	0.91	1.14
April	0.71	1.08
May	9.07	10.84
June	0.76	1.05
July	0.96	0.95
August	0.91	0.95
September	0.89	1.10

Company 13		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	31.38	47.73
November	29.59	48.33
December	34.23	47.34
January	28.78	45.99
February	36.91	50.52
March	36.34	49.74
April	37.20	50.96
May	30.97	46.68
June	29.16	43.21
July	29.83	48.18
August	30.93	45.98
September	30.87	44.50

Company 14		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	36.42	64.13
November	33.30	65.57
December	35.40	59.48
January	30.58	63.58
February	28.53	62.07
March	36.67	69.17
April	36.22	69.63
May	37.71	65.39
June	38.92	65.78
July	34.32	60.19
August	33.12	64.43
September	35.33	62.55

Company 15		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	19.13	81.75
November	22.66	89.60
December	25.41	71.64
January	23.47	86.63

February	23.40	86.59
March	23.48	86.65
April	23.22	75.84
May	18.83	77.55
June	20.54	96.32
July	19.40	84.43
August	20.67	87.81
September	22.50	84.52

Company 16		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	54.98	60.46
November	55.00	58.41
December	54.52	57.37
January	54.44	60.33
February	54.11	60.44
March	57.98	65.22
April	55.53	62.07
May	50.49	54.71
June	48.63	51.78
July	46.87	49.24
August	45.62	49.65
September	47.52	52.25

Company 17		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	8.49	16.41
November	10.36	15.73
December	10.80	17.17
January	11.61	16.79
February	8.20	16.68
March	8.81	17.14
April	8.75	18.87
May	9.27	19.00
June	9.73	21.01
July	9.26	19.32
August	10.23	19.87
September	9.57	18.83

Company 18		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	35.90	50.46
November	34.68	49.22
December	32.06	43.25
January	37.97	46.44

February	35.66	46.20
March	39.48	40.53
April	31.94	40.17
May	36.06	44.84
June	36.42	46.49
July	31.93	36.75
August	33.25	43.79
September	34.55	45.11

Company 19

Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	29.53	48.63
November	29.39	50.77
December	31.60	39.38
January	31.58	39.80
February	31.56	45.69
March	32.60	36.27
April	32.75	40.17
May	34.15	58.94
June	31.05	50.18
July	31.80	42.99
August	34.40	46.17
September	33.25	47.27

Company 20

Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	32.88	43.73
November	33.17	42.57
December	35.12	43.58
January	34.84	45.77
February	34.49	44.51
March	38.17	47.02
April	37.41	48.11
May	36.74	46.16
June	38.36	48.21
July	35.90	50.27
August	36.32	53.50
September	36.25	48.33

Company 21

Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	40.85	67.00
November	41.10	64.99
December	41.02	64.16
January	39.92	63.98

February	38.49	63.00
March	49.29	67.93
April	46.49	69.36
May	46.66	68.65
June	48.09	73.28
July	47.99	66.72
August	48.08	73.54
September	47.78	68.50

Company 22		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	5.68	34.04
November	6.03	28.67
December	6.21	26.81
January	6.63	34.44
February	7.23	30.72
March	6.61	31.79
April	6.91	73.95
May	6.77	70.07
June	6.58	37.22
July	6.00	29.62
August	6.67	25.77
September	6.75	35.44

Company 23		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	26.97	32.89
November	23.25	28.41
December	23.98	29.92
January	28.47	35.70
February	29.87	36.87
March	21.31	28.47
April	23.51	30.63
May	25.56	33.40
June	25.37	33.69
July	22.67	30.05
August	27.57	38.29
September	24.75	34.25

Company 24		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	37.69	56.54
November	31.03	52.11
December	31.03	50.59
January	32.98	55.36

February	28.05	50.57
March	26.24	50.47
April	29.46	45.54
May	24.08	38.29
June	21.97	33.90
July	20.15	35.20
August	17.55	30.13
September	22.25	35.22

Company 25		
Month	**Ingress Utilization (%)**	**Egress Utilization (%)**
October	32.09	49.42
November	31.29	50.69
December	30.42	44.91
January	31.24	46.96
February	31.99	51.93
March	29.67	45.10
April	28.31	42.80
May	27.09	45.24
June	28.66	44.20
July	31.10	40.25
August	28.05	46.45
September	27.55	45.53

The Infovista reporting tool allows exporting into different file formats, so the data was exported to Microsoft Excel and analyze. The analysis includes the mean, standard deviation, and circuit count for ingress and egress utilization for each company during the thesis timeframe. First, the mean and standard deviation was calculated for each month for all circuits, then the monthly results were used to calculate the mean and standard deviation for the one-year timeframe. The data for each company is in a separate Excel file and can be referenced as needed for future research and development. Only a synopsis of the data is included in the thesis because of the large volume produced for 29,675 circuits.

IV. Results and Explanation of Analysis

The analysis shows that every one of the companies have networks that are over provisioned. It was discussed in this thesis that one of the goals for network design is to maximize performance and availability and minimize cost. This does not meet the goal of minimizing cost. As an example, one company (16) has 4,234 circuits and the average inbound utilization is 52.56% and the average outbound utilization is 57.25% with standard deviations of 4% and 5.25%, respectively. The following table is a yearly synopsis of the data for the twenty-five companies analyzed.

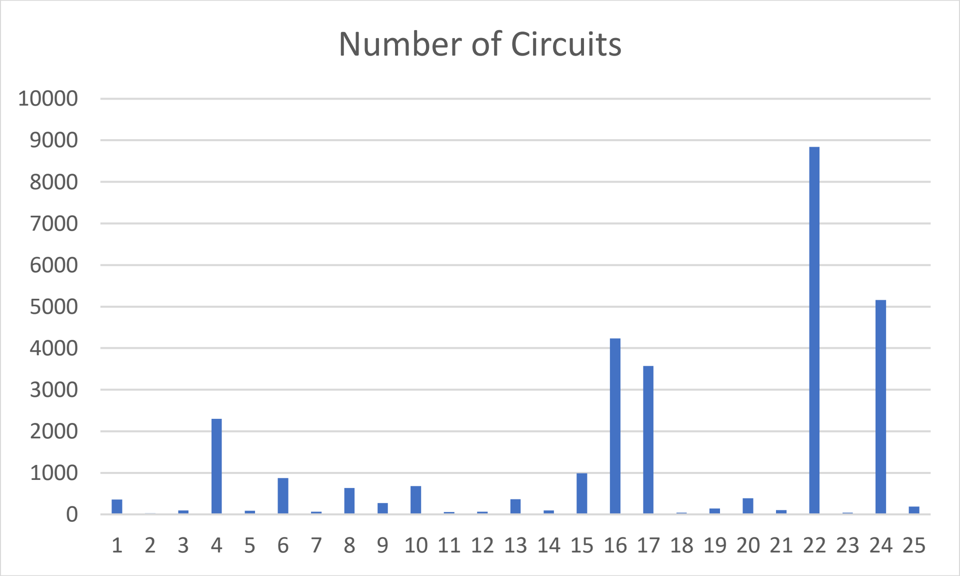
Table 4 Yearly Synopsis of Data

Company	**Number of Circuits**	**Inbound Utilization**	**Outbound Utilization**	**Inbound Std. Dev.**	**Outbound Std. Dev.**
Company 1	357	8.41	10.57	0.8	1.41
Company 2	27	16.23	20.66	4.52	7.6
Company 3	92	46.8	66.49	4.05	6.21
Company 4	2299	23.71	38.99	1.55	7.13
Company 5	86	11.79	15.38	1.5	1.81
Company 6	877	54.64	51.39	4.56	8.31
Company 7	63	9.34	7.23	2.57	1.67
Company 8	637	12.79	28.62	1.12	4.29
Company 9	272	37.97	49.96	1.28	3.21
Company 10	677	16.69	48.39	1.09	2.68
Company 11	54	23.22	34.35	3.06	4.92
Company 12	67	1.58	2.25	2.49	2.9
Company 13	364	32.3	47.7	3.25	2.25
Company 14	95	34.65	64.49	3.1	3.2
Company 15	991	21.84	84.07	2.2	6.96
Company 16	4234	52.56	57.25	4	5.25
Company 17	3568	9.59	18	1.06	1.68
Company 18	43	35.03	44.38	2.53	4.06
Company 19	142	31.86	45.36	1.59	6.56
Company 20	390	35.76	37.6	1.86	3.24
Company 21	106	44.36	67.51	4.04	3.55

Company 22	8845	6.48	38.46	0.45	16.94
Company 23	39	25.32	32.57	2.66	3.38
Company 24	5159	27.3	45.34	5.99	9.32
Company 25	191	29.99	46.18	1.73	3.45

The company names are changed for anonymity to protect proprietary information and are known only by the author of this study. The data shows a distribution for the number of circuits from small network environments to very large network environments. So, the proclivity to over provision seems to exist in this data no matter the size of the network. This is interesting because the companies were chosen randomly from the Fortune 500 list based on industry. We can assume each company has its own team with different engineers, so this seems to suggest an innate human trait with an inclination to over provision. There is a possibility these companies could have a consulting group in common and their design processes could lead to over provisioning. This may be a topic for future research and was not specifically covered by this study. The distribution for the number of circuits per customer is shown below.

Figure 3 Number of Circuits



The smallest network analyzed has 27 circuits (2) and the largest network has 8,845 circuits (22). Only one company (15) was above 80% for outbound utilization and no companies were above 80% for inbound. Two companies (6, 16) were above 50% for inbound utilization and six (3, 6, 14, 15, 16, 21) were above 50% for outbound. Typically, organizations would look at upgrading circuit bandwidth when sustained busy hour thresholds are in the range of 70% to 80% to stay ahead of the growth curve. Fifteen of the companies had inbound utilization less than 30% during busy hour measurements and seven had outbound utilization less than 30%, which is grossly over provisioned. As an example, if a company has a 100Mbps circuit provisioned, and they only need 10Mbps, that is an opportunity to save operational cost. A 100Mbps dedicated Internet circuit is around $1400.00 per month, whereas a 10Mbps circuit is $268.00 per month. That is an 81% savings on operating cost for a single circuit. If you multiple this example by thousands of circuits that is substantial savings. One company in our analysis (22) has 8,845 circuits. If this savings rate applies to all their circuits, that is over $10 million per month in operational savings. Even if it only applies to half of their circuits, that is still substantial savings for the organization. The inbound and outbound distributions are shown below.

Figure 4 Inbound Utilization

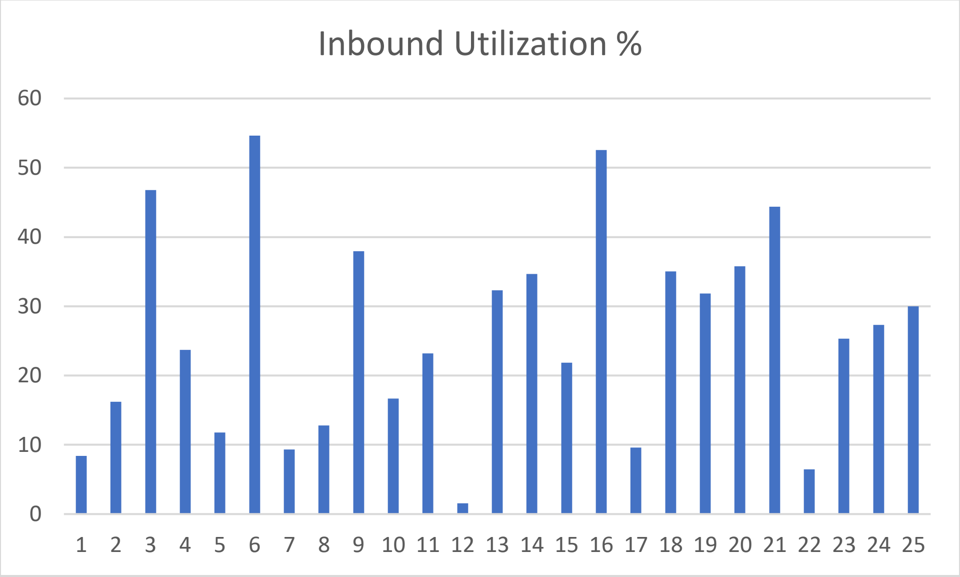
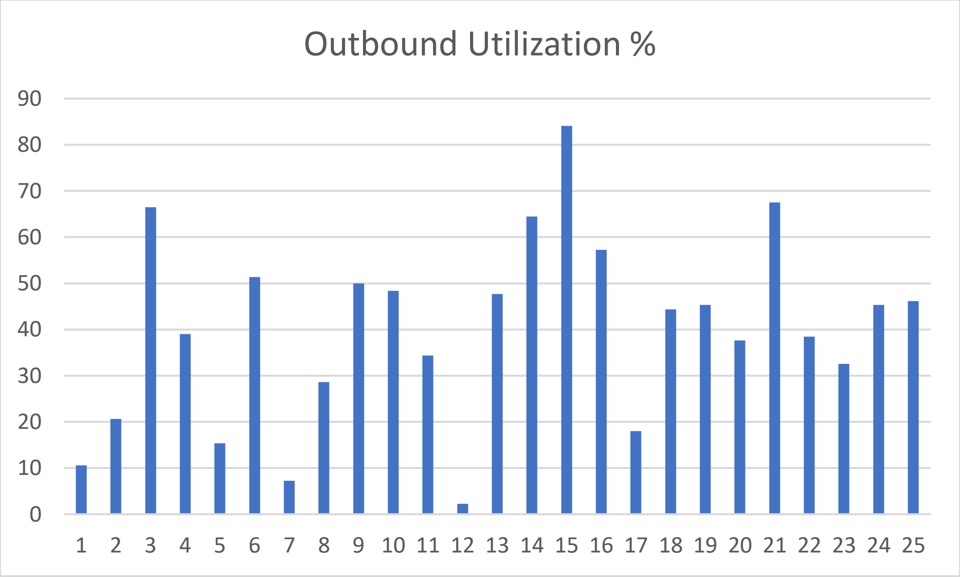


Figure 5 Outbound Utilization



The inbound and outbound utilization distributions show networks that are grossly over provisioned. In the raw data of each company, there were individual circuits that had peak utilizations of 99% and 100%, but this was very brief within a 15-minute timeframe and never occurred within the busy hour measurements. From this data it appears network engineers have designed their networks based on peak utilization, but this is not efficient and cost effective. Peak utilization is very bursty and only occurs for short periods of time. Even though circuits occasionally peaked at 100%, class of service profiles configured on the circuits would manage bandwidth for critical applications like IP voice and prevent performance issues. How many times have people experienced application issues and suspected the network? Network users, or even whole organizations will assume they need more bandwidth, but the data proves this is not an accurate assumption. This demonstrates we need to take a more holistic approach to what the application issues really are. Organizations must decide if networks provisioned for peaks in bandwidth utilization are worth the additional cost, especially when those peaks are typically less than five minutes. In large networks with thousands of circuits this is substantial.

Network engineers typically like to deal with known variables to determine bandwidth needs for specific locations. The following equation can be used to determine needs.

$$S = \sum_{x=1}^{N} a_x n_x$$

S is the total bandwidth required for a site, a is the per application bandwidth, and n is the number of users per application [110]. We know from earlier discussions this problem is NP-hard and this equation does not consider all the possible variables. We may not be able to determine all the variables in a given design, so if we follow this methodology for cloud environments, we could make the same mistakes. The data collected on twenty-five Fortune 500 companies shows too much bandwidth is being purchased to support the amount of traffic for each company. This has a negative impact on the operating expenses of each organization. These dollars could be redirected to research, development, or other initiatives to bring more value to stakeholders (investors, employees, owners, etc.).

As companies migrate to the cloud, they have the opportunity to utilize data to right size their network environments. Based on the collected data, this study recommends a scaling factor for the typical bandwidth equation. We cannot identify all variables needed to determine an equation to replace what we have, so data insights are one option. We have real world data from twenty-five companies, and when we examine the data, it shows all MNC's actual traffic needs are 40% to 60% of what they have provisioned. This is determined by yearly calculated mean and standard deviation. Therefore, a scaling factor of 0.4 to 0.6 is suggested for each environment. The bandwidth equation would become

$$S = (\beta) \sum_{x=1}^{N} a_x n_x$$

where β is the scaling factor for each site. Since service providers typically charge monthly fees for a fixed amount of bandwidth and services can be upgraded or changed as needed, this study would suggest starting with a factor of 0.5. By using NMSs to monitor connections, network administrators can determine if bandwidth should be adjusted and request change orders through the service provider's online portal. A scaling factor of 0.5 can be a baseline for designing the bandwidth needs for cloud services acting as a variable for unknown or undetermined data. Many unknown variables are involved in determining the required bandwidth for a given location including situations with the workforce such as work patterns of users, time spent in meetings, time on the phone, remote work away from the office, vacation and sick time, shift work and breaks, etc. The data insights collected by this study allows us to adjust bandwidth calculations to account for the unknown variables.

In addition, the data insights from this study will allow companies to design networks that are more diverse, providing more resiliency and availability at each site. Instead of over provisioning single circuits to each site, dual or even tertiary circuits can be provisioned at the same cost. Instead of a single dedicated Internet circuit, multiple diverse broadband circuits could be used for connectivity. This will allow network engineers to take full advantage of SD-WAN technologies by allowing the networking appliance to manage multiple circuits and select the best path for performance and availability. The savings from scaling bandwidth will also allow engineers to provide redundant SD-WAN equipment for failover, thus eliminating any single points of failure at the site.

V. Conclusions and Suggestions for Future Work

There has been a paradigm shift in technology where MNCs are migrating I.T. services to the cloud. This gives them the opportunity to right size their networks and not over provision Internet connectivity like they have with their private networks and DCs. This study collected utilization data on twenty-five Fortune 500 companies over a 12-month period to determine if existing network environments were designed efficiently. After analyzing the data, it has been determined all the companies are wasting operating capital by over provisioning network bandwidth.

There are too many variables to develop an effective equation to determine the amount of bandwidth required at each site, so this study is suggesting using data insights from existing networks to determine a baseline for designing and building networks for cloud services. One of the suggestions in this study is to add a scaling factor to the common equation used to determine required bandwidth. The results of the data analysis show a reasonable scaling factor is 0.5. Through the literature review no other works were found using real-world utilization data from twenty-five Fortune 500 companies to determine efficient bandwidth for cloud services. In addition, no other work has proposed a scaling factor for calculating bandwidth to account for unknown variables. Therefore, the analysis of real-world data from twenty-five companies and the proposed scaling factor is an original contribution from this work.

This study is just the beginning. One of the areas not addressed in this study is mobility and the impact it will have on cloud services. Many of the MNCs in this study have a mobile strategy as part of their overall network design. Unfortunately, this study did not have access to the mobile data to include in the analysis. One specific area of mobility worth investigating to expand on this study is how mobile edge computing (MEC) will affect the migration to the cloud. Cloud service providers are already working with mobile service providers to integrate MEC into the cloud. This will allow distributed cloud applications to be pushed closer to the users for better performance and availability. In addition, 5G NR will allow many more devices, speeds greater than 1 Gbps, and end-to-end network slicing. All of these features will play a vital role in how MNCs use cloud services.

Second, as companies migrate to the cloud, security becomes an integral part of the solution. Private networks and DCs have to address security at Internet access points in their environments. Many companies have centralized Internet access from DCs and backhaul all of their remote traffic through these protected connections. However, cloud migration based on Internet access makes every location vulnerable. Internet connectivity introduces phishing, viruses, DDOS, and other attacks into the network. It is important to understand how security affects cloud migration and what companies need to do to protect themselves.

Third, what is the best architecture for migrating to the cloud? Is it policy-based routing using traditional routers like we have been doing for several decades, or should we be using SD-WAN with SDN controllers managing the network? Either way we need to understand the role that machine learning and artificial intelligence will have in the cloud. AI engines can receive actionable data from the network elements and direct configuration and policy changes on routers or SD-WAN appliances. Applications can make direct API calls to the network to reserve required bandwidth end-to-end both from a wireless and wireline perspective and the AI can do the provisioning automatically. Can we get to zero effort networking where networks manage themselves?

Finally, does the results of the data analysis in this study apply in all situations? Twenty-five companies and 29,675 circuits are only the beginning. There are millions of companies in the United States and hundreds of millions around the world in different industries. We need to examine more data to see if the results of this study are accurate in all situations. This would require a collaboration between individuals who have access to NMS data at different telecom service providers. In addition, it would be interesting to collect more data from the specific sectors of each industry to determine if different scaling factors are required for a given sector. Two or three companies from each sector like the twenty-five companies in this study are not enough to determine if patterns exist per sector. To determine if different scaling factors are needed per industry, data would need to be collected and analyzed on twenty to twenty-five companies per sector. This would give a good indication of whether patterns exist within specific industry sectors.

The initial data from the twenty-five companies studied show a similarity across all these organizations. All these organizations have different teams of people with different engineers, and we can assume different genders and ethnicities. We would need to research this and collect data to determine for sure, but if this holds true, does it point to a human element for the over provisioned networks? Is there a concern, or fear of being blamed, innate within people? This would take more research, but if proven true, perhaps the only way to manage networks efficiently is through AI.

VI. References

[1] GlobalData, “GlobalData market opportunity forecasts to 2025: Cloud computing,” December 2021, https://technology.globaldata.com/Analysis/details/globaldata-market-opportunity-forecasts-cloud-computing, Accessed via web 1/26/2022.

[2] Cisco Press, “Campus LAN and wireless LAN solution design guide, pp. 64-76, May 2020, https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-campus-lan-wlan-design-guide.pdf, Accessed via web 1/26/2022.

[3] Floyd S. and Kohler E., “Internet research needs better models,” ICSI Center for Internet Research, Berkeley, CA., October 2002.

[4] C Di Cairano-Gilfedder and Clegg, R G. “A decade of Internet research – advances in models and practices,” BT Technology Journal Vol. 23, Issue 4, pp. 115-128, Oct 2005.

[5] Leland W E., Taqqu M S., Willinger W and Wilson D V., “On the self-similar nature of Ethernet traffic”, in Sidhu D P (Ed): ‘Proc ACM SIGCOMM’, pp. 183—193, San Francisco, CA, 1993.

[6] Taqqu M S., Willinger W and Sherman R., “Proof of a fundamental result in self-similar traffic modelling’, Computer Comm Rev, 27, pp. 5—23, 1997.

[7] Paxson V and Floyd S., “Wide-area traffic: the failure of Poisson modeling,” IEEE/ACM Trans on Networking, 3, pp. 226—244, 1995.

[8] Crovella M E and Bestavros A., “Self-similarity in the WWW traffic: evidence and possible causes,” IEEE/ACM Trans on Networking, 5, pp. 835—846, 1997.

[9] Feldmann A, Gilbert A C and Willinger W., “Data networks as cascades: investigating the multifractal nature of Internet WAN traffic,” Proc ACM SIGCOMM, pp. 42—55, 1998.

[10] Crane P., “A new service infrastructure architecture,” BT Technology Journal, Vol. 25, Issue 3-4, pp. 185-197, July 2007.

[11] 3rd Generation Partnership Project — http://www.3gpp.org/. Accessed via web 1/31/2022.

[12] Open Mobile Alliance — https://omaspecworks.org/. Accessed via web 1/31/2022.

[13] Botham, C P., Hayman, N., et. al., “Advanced modeling techniques for designing survivable telecommunications networks,” BT Technology Journal, Vol. 21, Issue 2, pp. 37-47, April 2003.

[14] Chamberland, S., “An analysis of three-level IP network topologies,” Canadian Conference on Electrical and Computer Engineering, 2007.

[15] Shameemraj M N., Vishvesh R., et al., “An enterprise Data Center network design – NetDes,” Fourth International Conference on Communication Systems and Network Technologies, 2014.

[16] Juan Li, Yan Qiao, et al., “An experimental design approach for link loss inference on large networks,” IFIP/IEEE International Symposium on Integrated Network Management, 2013.

[17] Chen Y, Bindel D, Song H, and Katz R H, “An algebraic approach to practical and scalable overlay network monitoring,” in Proc. ACM SIGCOMM, pp. 55–66, 2004.

[18] Chua D B, Kolaczyk E D, and Crovella M, "Efficient monitoring of end-to-end network properties," in Proc. IEEE INFOCOM, pp. 1701- 1711, 2005.

[19] Chua D B, Kolaczyk E D, and Crovella M, “A statistical framework for efficient monitoring of end-to-end network properties,” in Proc. ACM SIGMETRICS, pp. 390–391, 2005.

[20] Song H, Qiu L, and Zhang Y, “Netquest: A flexible framework for large scale network measurement,” IEEE/ACM Transactions on Networking, vol.17, no.1, pp.106-119, February 2009.

[21] Dustdar, S., Gall, H., “Architectural concerns in distributed and mobile collaborative systems, Parallel, Distributed and Network-Based Processing”, Proceedings of the Eleventh Euromicro Conference, pp. 475-483, February 2003.

[22] Kovachev, D., Cao Y., and Klamma, R. “Mobile cloud computing: A comparison of application models,” http://arxiv.org/pdf/1107.4940.pdf, Accessed via web 2/1/22.

[23] Kolici V, Xhafa F, et al., “Analysis of mobile and web applications in small and medium size enterprises,” Eighth International Conference on P2P, Parallel, Grid, Cloud, and Internet Computing, 2013.

[24] Segui Pascual V, and Xhafa F., “Evaluation of contact synchronization algorithms for the Android platform,” Mathematical and Computer Modelling 57, pp. 2895-2903, 2013.

[25] Freeman L C, “Centrality in social networks conceptual clarification,” Social Networks, vol. 1, no. 3, pp. 215–239, 2009.

[26] Etinkaya E K, Alenazi M J, Peck A M, et al., “Multilevel resilience analysis of transportation and communication networks,” Springer Telecommunication Systems Journal, 2013.

[27] Sterbenz J P, Hutchison D, Etinkaya E K, et al, “Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines,” Computer Networks, vol. 54, no. 8, pp. 1245–1265, 2010.

[28] Freeman L C, “A set of measures of centrality based on betweenness,” Sociometry, vol. 40, no. 1, pp. 35–41, 2007.

[29] Mohammed J F Alenazi, Egemen K Çetinkaya, et al., “Cost-constrained and centrality-balanced network design improvement,” 6th International Workshop on Reliable Networks Design and Modeling, 2014.

[30] “Industrial communication networks—High availability automation networks—Part 3: Parallel Redundancy Protocol (PRP) and High-availability Seamless Redundancy (HSR),” IEC 62439-3, International Electrotechnical Commission, 2010.

[31] Yazan M. Allawi, Dujeong Lee, et al., “Cost-effective topology design for HSR resilient mesh networks,” IEEE/OSA Journal of Optical Communications and Networking, Vol. 7, Issue 1, pp. 8-20, 2015.

[32] Tornatore M, Maier G, and Pattavina A, “Availability design of optical transport networks,” IEEE Journal Select Areas of Communication, vol. 23, no. 8, pp. 1520–1532, Aug. 2005.

[33] Kirrmann H, Weber K, Kleineberg O, and Weibel H, “Seamless and low-cost redundancy for substation automation systems (high availability seamless redundancy, HSR),” in Proc. IEEE Power and Energy Society General Meeting, pp. 1—7, July 2011.

[34] Whalley G M, Newson D J, et al., “Custom solutions for complex networks,” BT Technology Journal, Vol. 18, Issue 2, Apr 2000.

[35] Dijkstra E W, “A note on two problems connected with graphs,” Numerical Math, vol. 1, pp. 269—271, 1959.

[36] Dyer, C, “Testing router resource requirements with the OSPF routing protocol,” British Telecom, January 1999.

[37] Todd B and Doucette J, “Demand-wise shared protection network design and topology allocation with dual-failure restorability,” 11th International Conference on the Design of Reliable Communication Networks, 2015.

[38] Yuze He, Wei Li, et al., “ECCN: an elastic customized cloud network platform,” International Conference on Networking and Network Applications, 2016.

[39] McKeown N, "Software-defined networking." INFOCOM keynote talk 17.2, pp. 30—32 2009.

[40] Yeganeh, Soheil Hassas, Amin Tootoonchian, and Yashar Ganjali. "On scalability of software-defined networking." Communications magazine, IEEE 51.2, pp. 136—141, 2013.

[41] Paul Warren, John Davies, and David Brown, “End-to-end service level agreements for complex ICT solutions,” ICT Futures: Delivering Pervasive, Real-time and Secure Services, 2007.

[42] Carter S F, “Quality-of-service in BT’s MPLS-VPN platform,” BT Technology Journal, 23, No. 2, pp. 61—72, April 2005.

[43] J. Baliga, R. Ayre, et. al., “Energy consumption in optical IP networks,” Journal of Lightwave Technology, vol. 27, Issue 13, pp. 2391-2403, 2009.

[44] Lei Wang, Rui Lu, et al., “Energy efficient design and routing for IP over dynamic optical networks,” Asia Communications and Photonics Conference and Exhibition, 2010.

[45] Naoaki Yamanaka, Sho Shimizu, and Gao Shan, “Energy efficient network design tool for green IP/Ethernet networks,” 14th Conference on Optical Network Design and Modeling, 2010.

[46] Littlewood M, Gallagher I D, Adams J L, “Evolution towards an ATD multiservice network,” BT Technology Journal, Vol. 25, Issue 3-4, pp. 212-221, Jul 2007.

[47] B. Schroeder and G. A. Gibson, “A large-scale study of failures in high-performance computing systems,” Proceedings of the International Conference on Dependable Systems and Networks, Washington, DC, IEEE Computer Society, pp. 249–258, 2006.

[48] M. Kalyanakrishnam, Z. Kalbarczyk, and R. Iyer, “Failure data analysis of a LAN of Windows NT based computers,” Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, Washington, DC, IEEE Computer Society, pp. 178–187, 1999.

[49] D. Oppenheimer, A. Ganapathi, and D. A. Patterson, “Why do internet services fail, and what can be done about it?” Proceedings of the fourth conference on USENIX Symposium on Internet Technologies and Systems - Volume 4, Berkeley, CA, USENIX Association, pp. 1–15, 2003.

[50] L. J. Wilson, “Managing vendor relations: a case study of two HPC network issues,” Proceedings of the 24th international conference on large installation system administration, Berkeley, CA, USENIX Association, pp. 1–13, 2010.

[51] Jens Domke, Torsten Hoefler, and Satoshi Matsuoka, “Fail-in-place network design: interaction between topology, routing algorithm and failures,” Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis, 2014.

[52] Wittgreffe J P and Dames M P, “From desktop to data center -- addressing the OSS challenges in the delivery of network-centric ICT services,” BT Technology Journal, Vol. 23, Issue 3, pg. 65, July 2005.

[53] Wushu Ouyang, Horton Ai, et al., “Multi-layer IP Over Transport Network Design,” 22nd Wireless and Optical Communication Conference, 2013.

[54] Shirey R, “Internet Security Glossary,” IETF RFC2828, May 2000.

[55] L. He, “Recent developments in securing Internet routing protocols,” BT Technology Journal, Vol. 24, Issue 4, pp. 180-196, Oct 2006.

[56] Nessett D, “The internet security architecture,” Internet Security Workshop, IEEE, November 2014.

[57] Kent S and Atkinson R, “Security architecture for the internet protocol,” IETF RFC2401, November 1998.

[58] Kaufman E and Newman A, “Implementing IPsec: making security work on VPNs,” Intranets and Extranets, Published by John Wiley & Sons, Inc 1999.

[59] Heffernan A, “Protection of BGP sessions via the TCP MD5 signature option,” IETF Network Working Group, RFC2385, August 1998.

[60] M. Clouqueur and W. D. Grover, “Availability analysis of span-restorable mesh networks,” IEEE JSAC, vol. 20, pp. 810–21, May 2002.

[61] Manish Garg, J. Cole Smith, “Models and algorithms for the design of survivable multicommodity flow networks with general failure scenarios,” Omega, 36, pp. 1057-1071, 2008.

[62] Zhili Zhou, Tachun Lin, and Krishnaiyan Thulasiraman, “Survivable cloud network design against multiple failures through protecting spanning trees,” Journal of Lightwave Technology, Vol. 35, Issue 2, pp. 288-298, 2017.

[63] M. R. Rahman and R. Boutaba, “SVNE: Survivable virtual network embedding algorithms for network virtualization,” IEEE Trans. Netw. Serv. Manage., vol. 10, no. 2, pp. 105–118, Jun. 2013.

[64] Fei Teng and Gang Zhou, “The research of an approach to design local area network topology based on genetic algorithm,” Second International Symposium on Computational Intelligence and Design, 2009.

[65] Erik Joseph Seidel and Sonajie Wei, “‘The ZNSL network’: A novel approach to virtual networking,” International Symposium on Networks, Computers and Communications, 2019.

[66] S.A. Rouiller, “Virtual LAN security: weaknesses and countermeasures,” Technical report, SANS Institute, 2003.

[67] S. Narain, “Network configuration management via model finding,” Proc. Large Installations Systems Administration (LISA) Conference, 2005.

[68] Nihel Ben Youssef Ben Souayeh and Adel Bouhoula, “Towards safe and optimal network designs based on network security requirements,” IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[69] Yu-Wei Eric Sung, Xin Sun, Sanjay G. Rao, et al., “Towards systematic design of enterprise networks,” IEEE/ACM Transactions on Networking, Vol. 19, Issue 3, pp. 695-708, 2011.

[70] M Todd Gardner, Cory Beard and Deep Medhi, “Using network measure to reduce state space enumeration in resilient networks,” 9th International Conference on the Design of Reliable Communication Networks, 2013.

[71] Teare D, “Structuring and modularizing the network with cisco enterprise architecture,” Designing for Cisco Internetwork Solutions, Chapter 4, 2nd Edition, Cisco Press, Oct 12, 2007.

[72] Handley M, “Why the Internet only just works,” BT Technology Journal, Vol. 24, Issue 3, pp. 119 – 129, July 2006.

[73] Crocker S, “Protocol notes,” RFC 36, Network Working Group, Updated by RFC44, RFC 39, March 1970.

[74] Kudlick M, “Host names on-line,” RFC 608, IETF, January 1974.

[75] McQuillan J, Richer I and Rosen E, “The new routing algorithm for the ARPAnet,” IEEE Transactions on Communications, May 1980.

[76] Rosen E, “Exterior Gateway Protocol (EGP),” RFC 827, October 1982.

[77] Lougheed K and Rekhter Y, “Border Gateway Protocol BGP,” RFC 1105, June 1989.

[78] Kent S, Lynn C and Seo K, “Secure Border Gateway Protocol (SBGP),” IEEE JSAC Special Issue on Network Security, April 2000.

[79] Yuji Kojima and Kodo Ran, “Network design system recommending similar configurations characterized by manual knowledges,” 20th Asia-Pacific Network Operations and Management Symposium, 2019.

[80] IT, Juniper Networks, “The trouble that the network operator has in the survey of IT readers,” https://www.juniper.net/, May 2016. Accessed via web 2/15/22.

[81] Nanami Imada and Kazunori Ueda, “Peer-to-peer network system and application design on multiple virtual networks,” 19th International Conference on Network-Based Information Systems, 2016.

[82] Kreutz D, Ramos F M, Esteves Verissimo P, et al., “Software-defined networking: A comprehensive survey,” Proceedings of the IEEE, vol. 103, no. 1, pp. 14–76, 2015.

[83] Rowshanrad S, Namvarasl S, Abdi V, et al., “A survey on SDN, the future of networking,” Journal of Advanced Computer Science & Technology, vol. 3, no. 2, p. 232, 2014.

[84] O'Shea C D, “Strategic network topology and a capacity planning tool-kit for core transmission systems,” BT Technology Journal, Vol. 21, Issue 2, pp. 60-66, Apr 2003.

[85] Liu W, Sirisena H, et al., “Utility of algebraic connectivity metric in topology design of survivable networks,” 7th International Workshop on Design of Reliable Communication Networks, 2009.

[86] Mohar B, “Some applications of Laplace eigenvalues of graphs,” Graph Symmetry: Algebraic Methods and Applications, volume 497 of NATO ASI Series C, pp. 227-275, 1997.

[87] Fiedler M, “A property of eigenvectors of nonnegative symmetric matrices and its application to graph theory,” Czechoslovak Mathematical Journal, vol. 25, pp. 619–633, 1975.

[88] Fisher M A, “Virtualized computing infrastructure,” BT Technology Journal, Vol. 23, Issue 3, pp. 52-58, Jul 2005.

[89] Yun Li Shiying, Lei Qilie Liu, et al., “A cross-layer design for improving TCP performance in opportunistic networks,” 3rd IEEE International Conference on Broadband Networks and Multimedia Technology, 2010.

[90] Lindgren A, Doria A, and Schelen O, “Probabilistic routing in intermittently connected networks,” SIGMOBILE Mobile Computing Communications, Vol. 7(3), July 2003.

[91] Spyropoulos T, Psounis K, and Raghavendra C S, “Spray and wait: an efficient routing scheme for intermittently connected mobile networks,” SIGCOMM Philadelphia, P A, USA, Aug. 2005.

[92] Vahdat A and Becker D, “Epidemic routing for partially connected ad hoc networks. Technical Report CS-200006, Duke University, Apr. 2000.

[93] Allman M, Paxson V, and Stevens W, “TCP Congestion Control,” RFC 2581, Apr. 1999.

[94] Tamasi L, Orincsay D, et al., “Design of survivable VPN based VoIP networks,” 5th International Workshop on Design of Reliable Communication Networks, 2005.

[95] Grover W D, Zheng Y, "VP-based ATM network design with controlled over-subscription of restoration capacity," Design of Reliable Communications Networks, Brugge, Belgium, May 1998.

[96] Grover W D, Doucette J, Clouqueur M, et al., "New options and insights for survivable transport networks," , IEEE Communications Magazine, vol. 40, no. 1, pp. 34-41, January 2002.

[97] Lui X, Chandrasekhar S, and Winzer P, “Digital signal processing techniques enabling multi-Tb/s super channel transmission: An overview of recent advances in DSP-enabled super channels,” IEEE Signal Processing. Magazine, vol. 31, no. 2, pp. 16–24, Mar. 2014.

[98] “Spectral grids for WDM applications: DWDM frequency grid,” ITU-T Recommendation G.694.1, 2012, https://www.itu.int/rec/T-REC-G.694.1/en, Accessed via web 2/16/22.

[99] Gringeri S, Basch B, Shukla V, Egorov R, and Xia T, “Flexible architectures for optical transport nodes and networks,” IEEE Communication Magazine, vol. 48, no. 7, pp. 40–50, July 2010.

[100] Pedro J, “Designing transparent flexible-grid optical networks for maximum spectral efficiency,” Journal of Optical Communication Networking, vol. 9, no. 4, pp. C35–C44, Apr. 2017.

[101] Daniela Moniz, João Pedro, and João Pires, “Network design framework to optimally provision services using higher-symbol rate line interfaces,” IEEE/OSA Journal of Optical Communications and Networking, Vol. 11, Issue 2, pp. 174-185, 2019.

[102] Wes Chou, “Optimizing the WAN between branch offices and the Data Center,” IT Professional, Vol. 11, Issue 4, pp. 24-27, 2009.

[103] Pi´oro M and Medhi D, “Routing, Flow, and Capacity Design in Communication and Computer Networks,” Morgan Kaufmann Publishers, 2004.

[104] Srivastava S, Krithikaivasan B, Medhi D, and Pi´oro M, “Traffic engineering in the presence of tunneling and diversity constraints: Formulation and Lagrangian decomposition approach,” Proc. 18th International Teletraffic Congress (ITC18), Berlin, Germany, pp.461–470, 2003.

[105] Aubin R and Nasrallah H, “MPLS fast reroute and optical mesh protection: A comparative analysis of the capacity required for packet link protection,” Proc. Design of Reliable Communication Networks, Banff, Canada, pp. 349–355, 2003.

[106] Pan P, Swallow G, and Atlas A, “Fast reroute extensions to RSVP-TE for LSP tunnels,” IETF RFC 4090, May 2005. http://www.rfc-editor.org/rfc/rfc4090.txt, Accessed via web 2/17/22.

[107] Cotter R and Medhi D, “Survivable design of reconfigurable MPLS VPN networks,” 7th International Workshop on Design of Reliable Communication Networks, 2009.

[108] Burcu Barla Harter I, Schupke D A, et al., "Optimal design of resilient virtual networks," IEEE/OSA Journal of Optical Communications and Networking, Vol. 7, Issue 2, pp. 218-234, 2020.

[109] EMC, "EMC SMARTS Network Configuration Manager 9.6 Release Notes," January 2019, https://docs.vmware.com/en/VMware-Smart Assurance/9.6.0/EMC_Smarts_NCM_96_ReleaseNotes.pdf, Accessed via web 2/17/22.

[110] Scarpati J, "How to calculate network bandwidth requirements," TechTarget, https://www.techtarget.com/searchnetworking/tip/How-to-calculate-network-bandwidth-requirements, accessed via web 1/15/22.

VII. Appendix A – Sample Data File (Company 2)

10/1/2020 0:00	UTC								
			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed	Speed	Ingr Util	Ingr Util	Egr Util	Egr Util
				Ingr(Kbps)	Egr(Kbps)	BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	27.85	82.62	0.16	0.68
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	12.08	57.56	0.43	2.08
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	7.03	11.07	2.07	9.35
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	2.48	13.6	16.94	86.08
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	2.14	9.47	7.03	11.16
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.03	4.41	12.26	85.9
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.22	1.06	10.41	25.18
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.19	0.35	2.35	13.43
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.05	0.3	0.04	0.18
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	0.01	0.09	0.01	0.1
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	0.01	0.01	0	0

11/1/2020 0:00	UTC								
			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed	Speed	Ingr Util	Ingr Util	Egr Util	Egr Util

	String	String	Bandwidth	Ingr(Kbps) Bandwidth	Egr(Kbps) Bandwidth	BusyHr% Bandwidth	Peak% Bandwidth	BusyHr% Bandwidth	Peak% Bandwidth
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	76.14	84.06	56.36	99.56
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	70.7	83.2	16.74	38.37
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	28.71	85.32	2.5	9.43
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	28.25	41.24	28.82	85.37
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	13.4	15.46	9.1	22.57
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	9.14	10.65	15.45	58.27
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	5.1	6.95	4.35	6.65
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	4.37	19.23	16.99	69.06
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	4.07	6.5	4.82	6.87
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	3.95	8.04	42.13	89
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	2.18	3.88	6.05	15.95
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.06	4.35	18.33	53.07
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.18	0.35	1.55	11.89
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	0.13	1.34	0.08	0.2
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.11	0.29	8.45	31.89
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	0.06	0.36	0.48	2.8
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	0.01	0.01	0	0

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util	Ingr Util	Egr Util	Egr Util
						BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	84.27	92.43	88.19	100.77
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	38.78	87.39	53.67	99.87
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	29.02	82.75	1.01	5.3
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	24.87	90.25	37.54	98.69
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	18.39	20.56	10.96	30.98
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	14.03	37.81	83.92	98.12
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	8.64	11.68	32.34	66.06
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	3.47	18.71	25.59	79.05
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	1.5	8.83	0.91	9.13
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	0.98	2.58	6.39	14.44
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	0.48	2.48	0.76	4.38
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.45	1.25	0.42	2.54
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.34	1.98	0.18	0.86
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.26	3.11	2.83	8.5
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.18	0.42	3.82	12.03
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.12	0.51	6.22	35.31
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	0.1	0.21	0.34	3.78
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.1	0.22	9.4	61.2

1/1/2021 0:00	UTC								
			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util	Ingr Util	Egr Util	Egr Util
						BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	99.38	100.84	63.61	100.59
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	77.88	84.75	79.6	100.84
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	39.13	79.3	1.16	7.97
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	33.3	77.99	27.94	53.6
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	27.22	59.97	71.83	82.05
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	18.4	20.9	23.78	53.66
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	13.65	24.06	88.31	99.8
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	7.16	13.49	9.74	42.58
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	4.76	18.87	19.43	97.24
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	4.25	15.39	33.13	69.34
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	3.31	39.57	5.08	56.54
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	0.94	2.53	10.69	14.87
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	0.81	5.91	2.42	8.03
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	0.8	7.21	1	11.9
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.64	6.85	0.66	7.86
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.43	1.02	0.3	0.33

vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.31	2.2	4.97	13.26
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.24	0.59	6.98	27.31
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.1	0.25	0.14	0.39
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.09	0.2	11.95	32.67
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	0.05	0.13	0.09	0.28

2/1/2021 0:00	UTC								
			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed	Speed	Ingr Util	Ingr Util	Egr Util	Egr Util
				Ingr(Kbps)	Egr(Kbps)	BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	95.93	98.74	35.29	98.17
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	90.69	97.99	62.08	99.81
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	57.77	91.08	40.4	64.14
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	45.14	84.97	40.65	85.1
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	32.24	84.13	2.27	12.39
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	28.6	98.72	91.34	100.2
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	16.86	20.19	9.65	40.7
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	13.49	17.7	74.57	99.2
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	10.55	12.41	1.8	14.03
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	6.15	19.96	10.46	53.16
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	5.32	17.31	23.61	70.21

vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	4.49	16.67	6.57	25.23
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	4.39	20.24	54.44	93.47
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	2.29	2.46	7.06	16.31
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	2.26	9.55	11.94	40.1
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	1.49	17.79	0.32	2.27
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.43	2.4	3.8	12.57
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	1.1	2.27	2.13	4.77
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.57	0.97	0.58	0.6
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	0.22	2.38	4.26	47.94
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.13	0.35	0.11	0.2
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.09	0.18	3.85	30.65
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.07	0.21	2.81	32.67
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	0.01	0.1	0.01	0.05

3/1/2021 0:00 UTC

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed	Speed	Ingr Util	Ingr Util	Egr Util	Egr Util
				Ingr(Kbps)	Egr(Kbps)	BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	97.49	100.37	71.66	97.17
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	90.89	94.55	75.41	85.91
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	78.29	85.78	56.58	100.25

vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	58.43	97	61.35	100.52
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	49.19	89.01	70.99	87.39
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	31.01	82.79	2.56	11.29
vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.31	16.81	0.11	0.89
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	13.45	22.21	92.24	97.52
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	6.55	20	11.29	35.64
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	5.66	20.74	45.51	93.74
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	4.53	19.56	7.78	35.49
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	4.41	16.72	21.84	92.77
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	3.36	12.68	85.78	100.97
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	1.78	3.71	0.98	2.19
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	1.64	19.57	4.25	28.59
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	1.26	2.22	1.88	3.77
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	1.01	5.4	0.33	3.94
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	1	1.58	8.36	78.31
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	0.87	1.97	3.04	18.16
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	0.84	2.58	5.95	12.74
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	0.76	8.76	0.57	6.41
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	0.28	3.22	0.37	4.33
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.18	1.07	11.4	40.56
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.1	0.2	68.56	73.44

vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.08	0.24	0.29	0.75

4/1/2021 0:00 UTC

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util	Ingr Util	Egr Util	Egr Util
						BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	98.02	100.91	76.06	100.84
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	97.59	98.25	70.57	98.71
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	79.48	100.59	51.93	89.74
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	55.19	96.33	55.77	70.69
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	32.28	69.22	74.7	93.92
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	30.61	82.83	1.2	14.27
vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.39	17.22	0.06	0.37
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	13.36	16.48	92.4	98.37
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	8.42	19.38	34.22	83.52
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	6.87	46.94	24.01	54.18
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	5.71	10.17	13.06	88.59
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	4.34	19.92	75.46	87.16
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	3.5	12.75	64.41	98.67
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	3.25	14.12	15.31	18.91
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	2.29	24.31	1.64	5.69

vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	1.53	9.35	3.66	43.8
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	1.36	13.03	3.43	16.94
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	1.13	1.32	0.59	0.78
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	0.93	10.59	1.48	14.63
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.81	2.37	10.58	31.59
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.74	4.58	0.85	10.19
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	0.67	3.22	27.47	58.51
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.21	0.93	0.13	0.85
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.1	0.29	6.89	64.87
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.08	0.28	2.03	11.42

5/1/2021 0:00	UTC								
			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util BusyHr%	Ingr Util Peak%	Egr Util BusyHr%	Egr Util Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	94.83	100.38	99.78	100.81
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	67.38	95.9	35.73	95.76
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	62.18	99.58	85.34	99.8
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	43.22	88.14	71.42	80.9
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	38.29	83.07	0.76	9

vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	35.18	62.26	73.52	94.64
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	28.65	97.77	16.54	20.64
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	26.62	47.02	87.66	100.96
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	20.22	50.04	19.53	44.08
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	19.46	21.32	34.33	59.16
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	15.96	20.3	33.98	95.64
vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.48	31.16	1.8	21.58
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	14.05	17.03	13.11	60.5
vpn.eth.8477070.3790	BBEC.670740..ATI	WILLIAMSTON	ETH	10000	10000	12.52	23.92	42.22	99.87
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	11.05	20.39	13.96	39.23
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	8.21	50.21	14.32	48.9
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	6.17	12.74	4.51	32.73
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	5.61	52.22	51.38	100.84
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	1.82	10.11	3.86	22.21
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.49	4.3	18.02	69.37
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.71	1.83	0.58	1.86
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.52	2.53	10.34	24.05
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.32	1.59	0.23	1.66
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.25	1.76	0.22	2.59
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.09	0.2	8.23	30.29
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.08	0.28	0.52	1.15

6/1/2021 0:00 UTC

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util	Ingr Util	Egr Util	Egr Util
						BusyHr%	Peak%	BusyHr%	Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	10000	10000	93.46	100.35	82.42	100.87
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	76.04	81.57	2.64	31.5
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	61.26	96.78	50.4	98
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	50.13	87.55	9.21	21.55
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	47.75	99.8	89.98	99.14
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	41.74	92.95	71.3	94.34
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	37.24	94.41	66.41	93.76
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	30.12	42.65	88.12	99.56
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	24.48	42.55	17.25	57.92
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	17.09	20.29	12.93	65.26
vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.43	18.42	0.14	1.6
vpn.eth.8477070.3790	BBEC.670740..ATI	WILLIAMSTON	ETH	10000	10000	14.11	30.68	67.91	100.9
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	7.76	16.51	15.04	46.04
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	7.02	38.59	19.51	37.44
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	6.29	17.66	24.59	41.46
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	6.16	46.81	7.08	75.28
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	3.31	7.53	66.04	99.94
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	2.41	28.52	9.24	24.28

vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	1.2	3.05	1.63	8.58
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.2	3.72	11.55	19.46
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	1.03	12.16	0.36	3.79
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.84	1.07	0.57	0.76
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.78	7.67	1.76	19.57
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.21	0.56	0.11	0.26
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.18	0.56	3.65	35.96
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.08	0.19	0.25	1.02

7/1/2021 0:00 UTC

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed Ingr(Kbps)	Speed Egr(Kbps)	Ingr Util BusyHr%	Ingr Util Peak%	Egr Util BusyHr%	Egr Util Peak%
	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	20000	20000	85.29	88.97	62.1	98.55
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	83.33	99.69	69.26	98.69
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	46.43	70.53	84.18	94.82
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	44.17	90.11	71.01	85.33
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	42.54	95.73	75.61	100.6
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	37.89	62.23	12.57	50.67
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	30.52	81.2	22.35	94.81
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	20.12	20.77	23.17	77.38
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	16.36	29.4	85.36	100.27

vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.37	16.89	0.03	0.14
vpn.eth.8477070.3790	BBEC.670740..ATI	WILLIAMSTON	ETH	10000	10000	13.42	38.02	51.75	96.38
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	8.46	9.9	8.94	17.51
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	5.57	14.22	40.39	88.62
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	5.44	20.83	15.19	34.79
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	5.24	19.33	20.08	100.02
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	3.72	12.94	21.33	33.1
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	2.13	4.51	1.3	3.32
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	1.64	14.6	2.11	22.47
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	1.46	3.48	2.28	4.5
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.28	3.01	12.29	23.28
vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	1.27	15.18	6.22	74.51
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.72	2.68	1.61	11.54
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	0.62	0.96	11.34	26.05
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.58	5.4	3.21	21.4
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.09	0.21	11.07	54.65
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.08	0.18	0.25	0.77

8/1/2021 0:00 UTC

			b/s	kb/s	kb/s	kb/s	kb/s	kb/s	kb/s
MPLS Port ID	Access Circuit ID	CE Location	Protocol	Speed	Speed	Ingr Util	Ingr Util	Egr Util	Egr Util
				Ingr(Kbps)	Egr(Kbps)	BusyHr%	Peak%	BusyHr%	Peak%

	String	String	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth	Bandwidth
vpn.eth.8464739.2	IUEC.965989..ATI	COLUMBUS	ETH	50000	50000	93.71	100.27	93.5	99.05
vpn.eth.8471358.2	BBEC.674074..ATI	RENO	ETH	20000	20000	54.74	78.9	53.74	62.99
vpn.eth.8471663.2	IUEC.732460..ATI	COLUMBUS	ETH	30000	30000	52.25	94.38	69.04	95.52
vpn.eth.8461701.618	MMEC.947122..ATI	MANSFIELD	ETH	10000	10000	41.98	97.8	99.99	100.88
vpn.eth.8471662.2	MMEC.877284..ATI	COR	ETH	20000	20000	39.86	44.09	40.1	97.03
vpn.eth.8461859.744	BBEC.661150..ATI	GLEN ALLEN	ETH	20000	20000	31.55	82.55	3.13	37.36
vpn.eth.8471664.2	IUEC.813637..ATI	ORL	ETH	100000	100000	20.23	22.08	20.59	34.68
vpn.eth.8420618.2	IUEC.881333..ATI	COLUMBUS	ETH	100000	100000	19.7	21.59	11.3	50.69
vpn.eth.8487059.808	IUEC.979938..ATI	SHAKOPEE	ETH	100000	100000	15.52	16.96	0.06	0.29
vpn.eth.8491671.2	BBEC.666383..ATI	NAPRVL	ETH	10000	10000	14.31	16.9	92.09	95.1
vpn.eth.8477070.3790	BBEC.670740..ATI	WILLIAMSTON	ETH	10000	10000	13.28	34.28	34.42	96.57
vpn.eth.8514033.2	IUEC.918923..ATI	COLUMBUS	ETH	100000	100000	8.3	54.23	16.25	59.54
vpn.eth.8462666.1255	IUEC.899045..ATI	LEBANON	ETH	100000	100000	2.91	10.86	17.02	37.19
vpn.eth.8462986.2	BBEC.664473..ATI	PELHAM	ETH	20000	20000	2.89	13.94	57.17	83.77
vpn.eth.8517166.2	IUEC.710469..ATI	SPRINGFIELD	ETH	100000	100000	2.55	8.01	20.5	37.11
vpn.eth.8417863.421	IUEC.989118..ATI	HANOVER	ETH	40000	40000	2.14	25.47	1.06	9.79
vpn.eth.8425327.2	BBEC.544104..ATI	ROMEOVL	ETH	20000	20000	1.56	12.83	1.93	13.49
vpn.eth.8426299.2	IUEC.576165..ATI	ANH	ETH	100000	100000	1.19	4.21	5.15	25
vpn.eth.8420690.2	IUEC.751048..ATI	MORRISVL	ETH	100000	100000	1	3.7	22.57	87.94
vpn.eth.8424734	L4YS.946986..ATI	ASHBURN	ETH	10000000	10000000	0.86	1.08	0.68	0.77
vpn.eth.8421990.2	IUEC.925089..ATI	COR	ETH	100000	100000	0.45	2.83	0.2	1.95

vpn.eth.8463874.2	BBEC.674252..ATI	BUF	ETH	20000	20000	0.33	3.81	4.41	27.93
vpn.eth.8433657.420	IUEC.967922..ATI	HILLVIEW	ETH	100000	100000	0.32	0.47	3.88	28.43
vpn.eth.8464713.2	MMEC.574376..ATI	GRAND RAPIDS TWP	ETH	10000	10000	0.26	0.3	0.24	0.77
vpn.eth.8424587	L4YS.938730..ATI	RICHARDSON	ETH	10000000	10000000	0.14	0.37	0.13	0.28
vpn.eth.8464738.2	MMEC.581897..ATI	LENEXA	ETH	10000	10000	0.09	0.21	19.14	52.89