Authorization-based Approach for Customized Automated Resource Provisioning Services

Tananun Orawiwattanakul
National Institute of Information and Communications Technology
KDDI Building, 1-8-1 Otemachi, Chiyoda-ku, Tokyo, Japan, 100-0004
tananun@nict.go.jp

Hideki Otsuki
National Institute of Information and Communications Technology
KDDI Building, 1-8-1 Otemachi, Chiyoda-ku, Tokyo, Japan, 100-0004
eiji@nict.go.jp

Eiji Kawai
National Institute of Information and Communications Technology
KDDI Building, 1-8-1 Otemachi, Chiyoda-ku, Tokyo, Japan, 100-0004
eiji-ka@nict.go.jp

Shinji Shimojo
National Institute of Information and Communications Technology
KDDI Building, 1-8-1 Otemachi, Chiyoda-ku, Tokyo, Japan, 100-0004
sshinji@nict.go.jp

ABSTRACT

Combining the concept of software control with existing legacy network technology promotes new networking services with low capital expenditure. Currently, many testbeds and academic operators provide bandwidth on demand (BoD) services over layers 2 and 3 wide area network. BoD decreases operational expenditures and manual errors. However, administrators must continue to manually configure virtual circuits for different stakeholders to accommodate configuration conflicts, quality of service (QoS), and service policies. This paper proposes a BoD framework called AutoNET to provide a set of BoD services with independent abstract topologies, resource allocation, and different QoS levels. User authorization is employed to control the eligibility to access a given BoD service. AutoNET uses the extended On-Demand Secure Circuits and Advance Reservation System (OSCARS) as controller software and MultiProtocol Label Switching (MPLS) as a transport technology.

Keywords

Automated resource provisioning, bandwidth on demand, dynamic circuit network, quality of service.

1. INTRODUCTION

Bandwidth on Demand (BoD) in this paper refers to a service where the user can automate the creation, modification, and cancellation of a virtual circuit (VC) in advance. BoD is also called automated resource provisioning or dynamic circuit network (DCN). Currently, BoD software is deployed in many academic networks to ensure service agility at the production stage, e.g., AutoBahn, OpenDRAC, G-Lamda, OpenNSA, and the On-Demand Secure Circuits and Advance Reservation System (OSCARS) [1]. JGN-X [2], a Japanese new generation network testbed, provides transmission circuits on wide area network (WAN) (layers 2 and 3 (L2/L3)) for use in research and development of new generation network technologies. JGN-X utilizes OSCARS over MultiProtocol Label Switching (MPLS) networks for an L2/L3 BoD service called DCN. DCN in JGN-X efficiently supports applications that require high bandwidth, for example, data transmission by Virtualization-Node (V-Node) projects and e-learning. However, DCN cannot accommodate the policy conflicts of multiple stakeholders, because testbed users have different requirements.

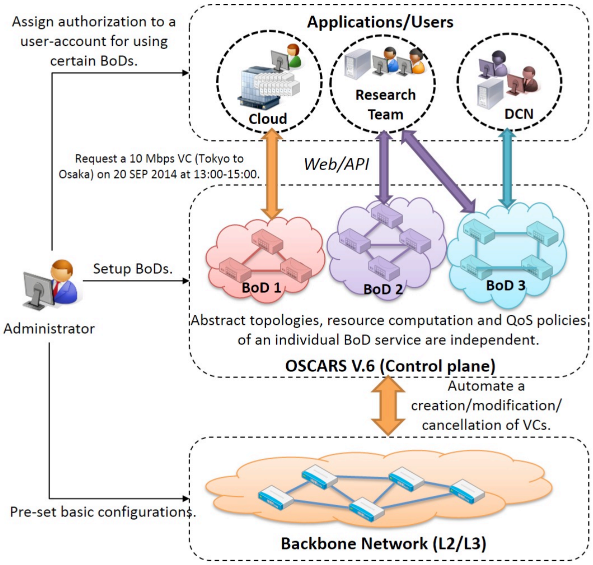
Assign authorization to a user-account for using certain BoDs.
Applications/Users
Cloud
Research Team
DCN
Request a 10 Mbps VC (Tokyo to Osaka) on 20 SEP 2014 at 13:00-15:00.
Web/API
Setup BoDs.
BoD 1
BoD 2
BoD 3
Administrator
Abstract topologies, resource computation and QoS policies of an individual BoD service are independent.
OSCARS V.6 (Control plane)
Automate a creation/modification/ cancellation of VCs.
Pre-set basic configurations.
Backbone Network (L2/L3)

Figure 1. AutoNET Framework.

For a concrete example, JGN-X provides a nation-wide OpenFlow network testbed called Research Infrastructure for large-Scale network Experiments (RISE) [3]. The RISE OpenFlow network has been operated on top of the same JGN-X L2/L3 backbone networks as DCN. Although using DCN can reduce the complexity and complete a set of network connections in a short period, the administrators manually configure switches to create an MPLS label-switched path (LSP) for connecting pairs of OpenFlow switches.

DCN cannot be used by the RISE team because of three areas of conflicts: (1) Quality of service (QoS): Flow rate restriction and call admission control (CAC) policies are applied in a DCN service, whereas RISE does not require input rate control for their LSP connections and the non-guarantee of QoS is acceptable. (2) Configuration: The RISE team requires pseudowire features and private node-ids in circuit configurations; these configurations are not used for DCN circuits. (3) Service-policy: The service topologies and maximum reservable bandwidth of DCN and RISE are different.

TRIDENTCOM 2015, June 24-25, Vancouver, Canada

DOI 10.4108/icst.tridentcom.2015.259705

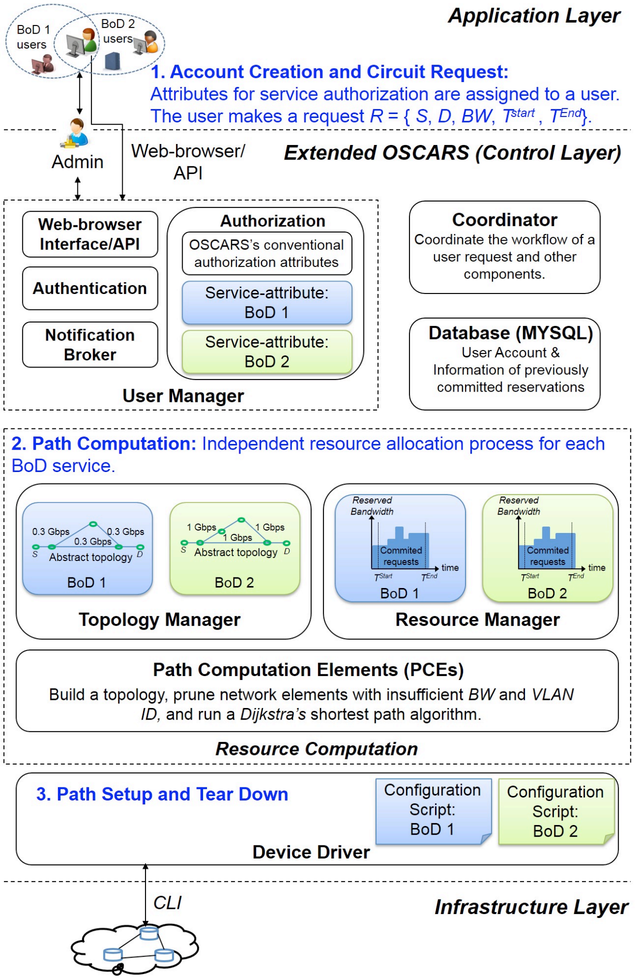
Application Layer
BoD 1 users
BoD 2 users
1. Account Creation and Circuit Request:
Attributes for service authorization are assigned to a user.
The user makes a request R = { S, D, BW, T^Start , T^End}.
Admin
Web-browser/ API
Extended OSCARS (Control Layer)
Web-browser Interface/API
Authentication
Notification Broker
Authorization
OSCARS's conventional authorization attributes
Service-attribute: BoD 1
Service-attribute: BoD 2
User Manager
Coordinator
Coordinate the workflow of a user request and other components.
Database (MYSQL)
User Account & Information of previously committed reservations
2. Path Computation: Independent resource allocation process for each BoD service.
0.3 Gbps
0.3 Gbps
0.3 Gbps
S
D
Abstract topology
BoD 1
1 Gbps
1 Gbps
1 Gbps
Abstract topology
BoD 2
Topology Manager
Reserved Bandwidth
Commited requests
time
T^Start
T^End
BoD 1
BoD 2
Resource Manager
Path Computation Elements (PCEs)
Build a topology, prune network elements with insufficient BW and VLAN ID, and run a Dijkstra's shortest path algorithm.
Resource Computation
3. Path Setup and Tear Down
Configuration Script: BoD 1
Configuration Script: BoD 2
Device Driver
CLI
Infrastructure Layer

Figure 2. Extended architecture of OSCARS v.6.

This paper proposes AutoNET, a framework to resolve the above conflicts by providing a set of BoD services with different abstract topologies, QoS, configurations, and service policies as depicted in Fig. 1. The authorization of a user account is used to identify a user's eligibility to access a given BoD service. The software and WAN technology used in AutoNET are extended OSCARS and MPLS, respectively. In AutoNET, OSCARS is extended to provide multiple BoD services, and a combination of QoS mechanisms performed by OSCARS and switches is used to achieve QoS differentiation among BoD services. Section 2 presents related work. Sections 3 and 4 describe the approach, controls, and infrastructure. Experiments are discussed in Section 5. The paper is concluded in Section 6.

2. RELATED WORK

The objective of AutoNET is to provide multiple BoD services over L2/L3 switches allowing QoS and service policies to be customized to groups of users. Clean-state-design technologies, e.g., Software-Defined Network（SDN）and Network Functions Virtualization (NFV), can provide full network virtualization, and several slicing dimensions can be virtualized, such as topology, bandwidth, device processing units, forwarding tables, and flow spaces. However, this paper focuses on L2/L3 networks, because most of production BoD services run on L2/L3 WAN networks.

Several groups of users utilize JGN-X networks with different requirements especially QoS, and multiple classes of QoS provisioning should be provided. Several techniques have been proposed for QoS guarantee in BoD. The layer 1 BoD service in Science Information NETwork (SINET) [4] can provide bandwidth and delay guarantee over optical networks; however, the majority of production BoD services deploy L2/L3 technologies. The Application-Layer Traffic Optimization (ALTO)–based virtual private network (VPN) topology manager in [5] provides on demand VC provisioning. It uses the real time status of a network to recommend a path that can satisfy the given constraints including bandwidth and delay. However, this real time mechanism cannot commit a QoS guarantee of data transmission for a future time.

In [6], pooled resources of LSPs and pseudowire in MPLS-Transport Profile networks are set in advanced, and the controller manages their status and allocates those unused to the users. However, the resource-pooling mechanism is not sufficiently flexible to provide several constraint path computations and multi-QoS levels. The studies in [7] determine the proper QoS mechanisms in L2/L3 switches to achieve high throughput for the high-rate traffic flows while reducing delay in real-time flows. In our previous work [8], CAC, bandwidth policing, and scheduling disciplines were used to provide bandwidth and delay guarantees in an MPLS-based BoD service. The QoS used in AutoNET is based primarily on the mechanisms used in [8].

3. ARCHITECTURE OF EXTENDED OSCARS (CONTROL LAYER)

OSCARS was extended to provide a set of BoD services. When creating a BoD service, the administrator assigns the virtual topology data and mapped physical devices, configuration files, and QoS level for an individual BoD service. A user can request a VC only from authorized BoD services. For simplicity, it is assumed that two BoD services are provided: BoD 1 and BoD 2. Figure 2 presents the high-level architecture of the proposed extended OSCARS. OSCARS consists of several web service modules that can be classified into five main groups: user manager, resource manager, device driver, coordinator, and database (MySQL). The process of circuit creation can be described as follows.

3.1 Account Creation and Circuit Request

OSCARS provides web-browser and application programming interfaces (API) to interact with the users, either humans or applications. The user must register for an account for authentication (using a user name and password for web-browser access and a distinguished name for API access).

OSCARS includes its own local authentication system and user information is stored in the MYSQL database. The administrator can assign an account either through a web page or directly through MYSQL. When creating an account, the administrator assigns authorization attributes to the user account. Upon user authentication, OSCARS uses the authorization attributes to determine the actions this user can perform in a local domain. For example, the "OSCARS-USER" attribute refers to the authorization to request a circuit. Complementing the authorization attributes in conventional OSCARS, we extended OSCARS by adding new authorization attributes called service-attributes. These new attributes are used to identify users who are authorized to use the BoD resources. Two service-attributes are created for authorization to use BoD1 and BoD2: 1. Name: jgn-x-

BoD1 and Value: "BoD1", 2. Name: jgn-x-BoD2 and Value: "BoD2", respectively.

A user can be authorized to use multiple BoDs by assigning corresponding service-attributes to the user account. Upon successful user authentication, the user requests a circuit. The request R can be described as R = [source (S), destination (D), amount of bandwidth (BW), start time (t^{Start}), end time (t^{End})]. The OSCARS requests contains *OptinalConstaint* attributes, and the researchers/developers can add new constraints in these attributes. OSCARS was extended to determine the user account and add the service-attributes into the *OptinalConstaint* attributes in the request for use in other modules.

3.2 Path Computation

Topology data are assigned to each BoD service and stored in the Topology Manager. OSCARS uses the schema defined by the Open Grid Forum/network-monitoring working group to describe the topology data. Each network element including the source and destination names is presented using a Uniform Resource Name (URN) beginning with the prefix "urn:ogf:network" and contains the parent elements' ID according to the hierarchy structure. We use an annotation of the node name to distinguish the resources of each BoD service. The prefix of the node name contains the constraint value of the corresponding service attribute-value. For example, a link ID of BoD1 "urn:ogf:network:domain=testdomain-1:node=BoD1-1:port= port1:link=link1" contains a domain ID, a node ID (the prefix is the value of the corresponding service name "BoD1"), a port ID, and a link ID. The Coordinator in OSCARS was extended to check the prefix of the node names of the source and the destination to determine a corresponding BoD service. It then checks the service-attributes of the requester to determine whether the requester is authorized to use this BoD service. The request is rejected if the requester is not authorized.

OSCARS uses multiple path computation elements (PCEs) to compute a path. Note that topology data contain the link capacities and a range of VLAN ids. First, the PCEs build the topology content. Then, the PCEs perform CAC by pruning links with insufficient bandwidth for BW during the requested transmission period (from t^{Start} to t^{End}). The resource manager records the details of previously committed requests including source, destination, requested bandwidth, and the assigned path. Because the network elements of BoD services are uniquely annotated, the available resources in each link in each service can be independently computed. Next, the PCEs prune the links with insufficient virtual local area network identifier (VLAN id). Finally, the end-to-end path is computed based upon Dijkstra's shortest-path algorithm. If there are sufficient resources, OSCARS updates the resource manager database with the new reservation information.

3.3 Path Setup and Tear Down

OSCARS consists of several device drivers, e.g., EoMPLSPSS, StubPSS, OpenFlowPSS, and DragonPSS. In this paper, the device driver referred to is EoMPLSPSS, which supports several L2/L3 vendor-routers, e.g., Cisco and Juniper. The device driver configures the circuit based on the configuration scripts. Although the administrator can write any script for any transport technology, the default template is based on MPLS configurations. This paper also uses MPLS because it provides carrier-grade QoS support. The device driver maps the virtual topology data to the physical devices by mapping the node-name contained in the topology data to the IP address of the corresponding switches based on the administrator's setting. It discovers devices in its domain through IP addresses. Because the names of node elements in BoDs are unique, they can be mapped to any IP address.

OSCARS periodically checks the database to select a request and communicates with the switches to perform the proper tasks, i.e., creating, modifying, or deleting VCs. Multiple configuration-script files for circuit creation, modification, and cancellation are predefined in OSCARS for each BoD service by the administrator. We extended OSCARS to select configuration files base up on a corresponding BoD service to set up and tear down an MPLS LSP before t^{Start} and after t^{End}, respectively. Resource ReserVation Protocol (RSVP) is used to establish explicitly routed LSPs based on OSCARS's computed path. Section 4 provides additional details regarding the infrastructure setting.

OSCARS can interoperate with other controllers through either the Inter-Domain Controller Protocol (IDCP) or the Network Service Interface (NSI) 2.0 for inter-domain communications. Presently, our proposal supports multiple intra-domain BoD services, while only a single BoD service can provide inter-domain circuits.

4. MULTI-QOS PROVISIONING IN THE INFRASTRUCTURE LAYER

The QoS level in this paper is committed for a request-flow at the time that a user requests a circuit, even if the actual transmission is scheduled for the future. Sections 4.1 and 4.2 describe QoS mechanisms and a QoS setting guideline for different QoS levels, respectively.

4.1 QoS mechanisms

Three QoS mechanisms are used in this paper: CAC performed by OSCARS, scheduling discipline, and bandwidth policing performed by the routers (available in most major-vendor routers).

Call Admission Control (CAC): As described in the Section 3.2, the PCEs in OSCARS perform a CAC mechanism to ensure that the total committed bandwidth of each BoD is not greater than the capacity described in its topology data.

Scheduling discipline: The administrator presets the resources of the virtual queues in the routers. The capacity of the egress queue of the Ethernet interface can be partitioned to a set of virtual queues. Three main parameters are generally assigned to a virtual queue: an assigned transmit rate, a percentage of the buffer size, and a priority.

Bandwidth policing: Classification is a mechanism that assigns to which virtual queues packets should be forwarded. Typically, the administrator configures the classifications that are available for a specific port, e.g., Ethernet level 802.1p or MPLS EXP/TC bits for layer 2, or DSCP, IP precedence, or 802.1p for layer 3. A firewall filter is a mechanism that can be used to overwrite the general classification of packets to assign the proper queues based on a specific BoD policy.

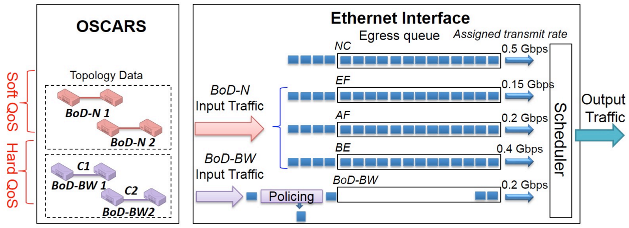

Figure 3. Scheduling in routers.

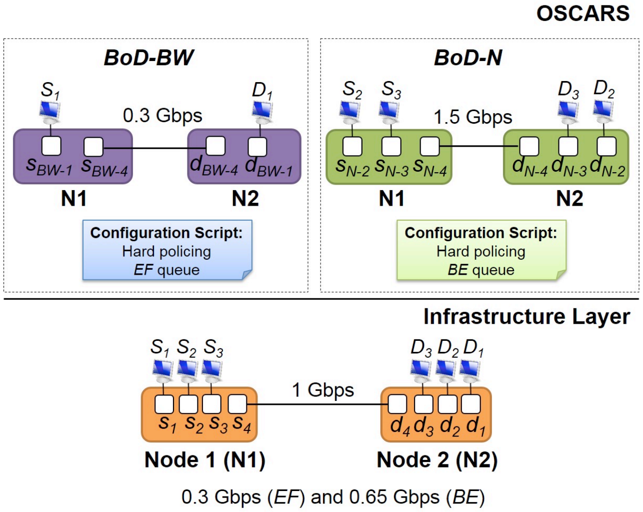

Figure 4. Network topologies used in experiments.

These queue assignment (firewall filter) policies can be written in configuration scripts and assigned on a request-flow basis as follows:

Without rate control: All packets of a flow are forwarded to a specific virtual queue.

With rate control: Bandwidth policing is performed at the ingress interface and it determines whether the input traffic of a data flow complies with the requested bandwidth *BW*. Because an individual virtual queue cannot be assigned to an individual flow, a rate limit is essential to protect the shared resources to maintain the performance for users that honor their contracts. Bandwidth metering is based on the token bucket algorithm, e.g., a single-rate two-color (srTC), single-rate three-color (srTCM) (RFC2697), and two-rate three-color (trTCM) (RFC2698). Note that SrTC is used in our experiments (Section 5). The bandwidth policer monitors the sending rate of a traffic flow. It forwards the in-profile packets (traffic under *BW*) to a specific queue. If the input traffic exceeds *BW*, two actions can be performed: 1. Discard excess traffic (called out-of-profile packets); 2. Reclassify out-of-profile packets to another queue. The former action is called hard-policing; the latter is called soft-policing.

Virtual queues and their resource allocations are preconfigured in the routers, whereas bandwidth policing and firewall filter are established by OSCARS through the administrator's prewritten configuration scripts.

4.2 QoS Setting

In this proposal, each BoD service can provide different QoS classes. Note that QoS mechanisms for delay guarantee and minimum delay path computation are presented in our previous work [8]. In this paper, two classes are described: no guarantee of QoS (*BoD-N*) and guarantee of bandwidth (*BoD-BW*).

BoD-N: There is no strict guarantee of QoS; however, soft QoS mechanisms such as Differentiated Services (DiffServ) [9] may be used. Default forwarding classes and their associated queues, i.e., best-effort (*BE*), expedited forwarding (*EF*), and assured forwarding (*AF*) are generally used in DiffServ. Input rate-control in bandwidth policing is an option. It is not necessary that the actual allocated resources in the switch topology are associated with the corresponding virtual topology in OSCARS. Overbooking in CAC can be performed by assigning link capacity in the abstract topology over the capacity in the infrastructure layer.

BoD-BW: This class offers a guarantee of the user's requested bandwidth *BW*. Input rate-control in bandwidth policing is mandatory. The new virtual queue (the *BoD-BW* queue in Fig. 3) may have to be created in addition to the default queues such as *EF*, *BE*, and *AF* if they are used by other traffic. Note that the LSP is established in the infrastructure layer based on the OSCARS's computed path. No overbooking in CAC is allowed. The allocated transmit rate of an egress queue in a physical interface is associated with a capacity of a corresponding link in an abstract virtual topology in OSCARS. For example, two *BoD-BW* services are provided on a single link network with 1 Gbps capacity in Fig. 3. The summation of the link capacities in the abstract topologies of the *BoD-BW1* and *BoD-BW2* services in OSCARS must be equal to or less than 0.2 Gbps, i.e., $C1 + C2 \leq 0.2$ Gbps. A combination of CAC and rate control ensures that the total input rate into a corresponding queue does not exceed the queue transmit rate.

5. EXPERIMENTS

This section presents the experiments performed to verify that the proposed prototype can provide multiple BoD services with QoS differentiation. Figure 4 illustrates the network topology used in an infrastructure layer and the proposed extended OSCARS.

The infrastructure layer: Experiments were performed on a Juniper MX-80 running Junos v.12.3. We used the logical system capability of a MX-80 router to build a single-link network as indicated in the infrastructure layer in Fig. 4. Several configurations, e.g., RSVP, Label Distribution Protocol (LDP), and Open Shortest Path First (OSPF) were preconfigured in the routers. Let S_i - D_i denote the pair of source and destination hosts, and s_i and d_i denote their corresponding ports, respectively. All ports have the same capacity, 1 Gbps.

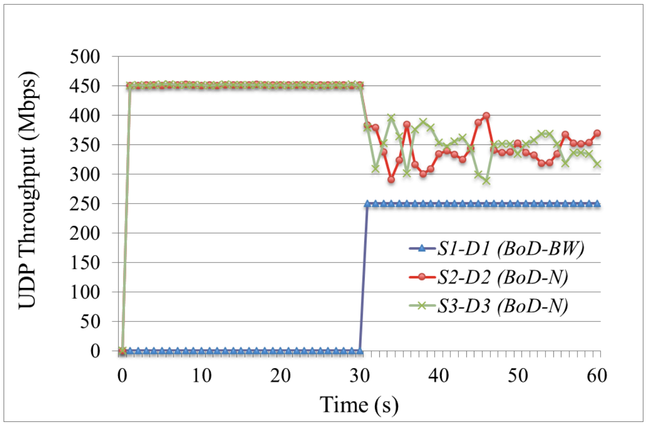

Figure 5. UDP throughput of *BoD-BW* and *BoD-N* flows.

Three virtual queues were defined at the egress queue of the interfaces s_4 and d_4: *BE*, *EF*, and network control (*NC*). A set of the assigned transmit rates, a percentage of the buffer size, and priority { 0.65 Gbps, 65%, "medium-high" }, { 0.3 Gbps, 30%, "medium-high" }, and { 0.05 Gbps, 5%, "medium-high" } were assigned to the *BE*, *EF*, *NC* queues, respectively. Note that the transmit rate was shared among virtual queues in work-conserving mode (unused bandwidth of any queue can be shared with other queues.)

OSCARS: Two BoD services with *BoD-BW* and *BoD-N* QoS provisioning were provided on the same routers. The abstract topologies for both BoD services were added to the proposed extended OSCARS and were annotated as described in Section 3. For simplicity, $s_{BW\text{-}i}$ and $d_{BW\text{-}i}$, and $s_{N\text{-}i}$ and $d_{N\text{-}i}$, denote the corresponding physical ports s_i and d_i in the *BoD-BW* and *BoD-N* services, respectively. The configuration scripts for the circuit-creation of the *BoD-BW* and *BoD-N* services were written to contain srTC, hard-policing and firewall filter commands to redirect in-profile traffic to the *EF* and *BE* queues, respectively. In srTC, the user's requested bandwidth *BW* is set as the token rate; a maximum burst size (10% of BW) is used to limit the number of tokens in a bucket. The link capacity in the abstract topology of the *BoD-BW* service in OSCARS must associate with the assigned transmit rate of the *EF* queue, i.e., 0.3 Gbps in our experiments (see Fig. 4). Combining SrTC and hard-policing with the CAC performed by OSCARS, the input traffic entering the *EF* queue did not exceed 0.3 Gbps. For *BoD-N*, we performed overbooking in our experiments; 1.5 Gbps in the abstract topology whereas only 0.65 Gbps was assigned to its corresponding *BE* queue.

5.1 QoS Differentiation

We created a user account with authorization to use both *BoD-BW* and *BoD-N* services and used this account to request three VCs: {$s_{BW\text{-}1}$, $d_{BW\text{-}1}$, 280 Mbps}, {$s_{N\text{-}2}$, $d_{N\text{-}2}$, 450 Mbps}, and {$s_{N\text{-}3}$, $d_{N\text{-}3}$, 450 Mbps}. Note that the request is described as {the source, the destination, requested BW}; the start and the end times cover the entire experiment period. Six computer hosts S_1, S_2, S_3, D_1, D_2, and D_3 were connected to the ports s_1, s_2, s_3, d_1, d_2, and d_3 of the router, respectively. The traffic of the S_1-D_1 flow, which does not exceed 280 Mbps, should be guaranteed (*BoD-BW*), whereas there is no bandwidth guarantee for the S_2-D_2 and S_3-D_3 flows (*BoD-N*). All hosts ran Iperf v.2.0.5 for the user datagram protocol (UDP) traffic generation with a 1,470 byte datagram size. The S_2-D_2 and S_3-D_3 flows transmitted data at the rate 450 Mbps (total 900 Mbps) from time zero to time 60 s. The S_1-D_1 flow was initiated at time 30 s to transmit data at the rate of 250 Mbps until time 60 s. In this scenario, only the link s_4 to d_4 congested.

Figure 5 presents the UDP throughput obtained from the Iperf reports. From time zero to 30 s, the throughput of S_2-D_2 and S_3-D_3 achieved their sending rate because the unused bandwidth of the *EF* and *NC* queues could be utilized by the *BE* queue. As the traffic of the S_1-D_1 flow increased, the throughput of the S_2-D_2 and S_3-D_3 flows each rapidly decreased to approximately 350 Mbps as indicated in Fig. 5. Because the S_1-D_1 flow rate at 250 Mbps was in-profile, its throughput was at it sending rate. The total throughput from the Iperf report did not equal 1 Gbps, because of network overhead, e.g., an MPLS header. This experiment verifies that the requested *BW* can be guaranteed for the *BoD-BW* flow.

6. CONCLUSIONS

Users in testbeds have different requirements for transmission circuits, e.g., configurations and QoS. This paper proposes a BoD framework called AutoNET. AutoNET added flexibility and customizability into OSCARS to tailor network services to the specific needs of users. Our framework enables an administrator to customize a BoD service to satisfy certain requirements for a group of users, such as service area, QoS, and configurations. In this paper, we briefly describe a QoS setting guideline for L2/L3 switches for QoS differentiation among BoD services. AutoNET decreases workload of administrators and communication time between users and administrators. Our future work includes features that enable authorized *BoD-N* users to control packet classification in DiffServ and provide multiple classes of QoS in an individual BoD service.

7. REFERENCES

[1] On-Demand Secure Circuits and Advance Reservation System (OSCARS). Retrieved: 19.1.2015. [Online]. Available: http://www.es.net/services/virtual-circuits-oscars

[2] JGN-X. Retrieved: 19.1.2015. [Online]. Available: http://www.jgn.nict.go.jp/english/

[3] Y. Kanaumi, S. Saito, E. Kawai, S. Ishii, K. Kobayashi, and S. Shimojo, "RISE: A Wide-Area Hybrid OpenFlow Network Testbed," IEICE Transactions 96-B(1), pp. 108-118, 2013.

[4] S. Urushidani, K. Fukuda, Y. Ji, S. Abe, M. Koibuchi, M. Nakamura, and S. Yamada, K. Shimizu, R. Hayashi, I. Inoue, and K. Shiomoto, "Resource Allocation and Provision for Bandwidth/Networks on Demand in SINET3," in Proceedings of the IEEE Network Operations and Management Symposium Workshops (NOMS), 2008, pp. 212 – 218.

[5] M. Scharf, V. Gurbani, T. Voith, M. Stein, W. Roome, G. Soprovich, and V. Hilt, "Dynamic VPN optimization by ALTO guidance," in Proceedings of the 2nd European Workshop on Soft-ware Defined Networks (EWSDN), 2013, pp. 13–18.

[6] T. Iijima, T. Suzuki, K. Sakamoto, H. Inouchi, and A. Takase, "Applying a Resource-pooling Mechanism to MPLS-TP Networks to Achieve Service Agility," in Proceedings of the 5th International Conference on Cloud Computing, GRIEs, and Virtualization (CLOUD COMPUTING), 2014, pp. 31-36.

[7] Z. Yan, M. Veeraraghavan, C. Tracy, and C. Guok, "On How to Provision Virtual Circuits for Network-Redirected Large-Sized, High-Rate Flows," in Proceedings of the International Journal on Advances in Internet Technology, vol .6, no. 3&4, 2013.

[8] T. Orawiwattanakul, H. Otsuki, E. Kawai, and S. Shimojo, "Multiple Classes of Service Provisioning with Bandwidth and Delay Guarantees in Dynamic Circuit Network," in Proceedings of the 14th IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2015.

[9] F. Le Faucheur, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval, and J. Heinanen, Request for Comments (RFC): 3270, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services." Available: https://www.ietf.org/rfc/rfc3270.txt