gwg
Internet Draft
Intended status: Informational
Expires: September 11, 2019

S. Wadhwa
K. DeSmedt
P. Muley
Nokia
R. Shinde
Reliance Jio
J. Newton
Vodafone
R. Hoffman
TELUS
S. Pani
Juniper Networks

March 11, 2019

Requirements for Protocol between Control and User Plane on BNG
draft-wadhwa-rtgwg-bng-cups-protocol-requirements-02.txt

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on September 11, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

Traditionally, the BNG provides aggregation of fixed access nodes (such as DSLAM and OLTs) over Ethernet and provides subscriber management and traffic management functions for residential subscribers. The BNG has however evolved to become a multi-access edge device that also provides termination of subscribers over fixed-wireless and hybrid access. An overall architecture and interfaces required between separated control and user-plane for a multi-access BNG are described in draft-wadhwa-rtgwg-bng-cups-01.txt. This document discusses requirements for protocol between subscriber-management control-plane and user-plane for BNG to achieve separation.

Contents

1. Introduction

This document describes a set of requirements for protocol between subscriber-management control and user plane for BNG, that need to be met, in order to achieve separation. In rest of the document the control plane is referred to as CP, user plane as UP, and the separation is referred to as CUPS (control and user plane separation). The protocol between control and user-plane to achieve separation is referred to as "CUPS protocol". These requirements should form the basis for "CUPS protocol" selection. The functional decomposition between CP and UP, and applicability of CUPS to a BNG that can support multiple access technologies such as fixed (DSL or Fiber), fixed-wireless (LTE,5G) and hybrid access are described in [CUPS].

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Requirements for "CUPS protocol"

[CUPS] defines overall operation and architecture for control and user-plane separation on BNG. It also defines key functional interfaces between CP and UP, as shown in Fig 1, to realize the separation. "CUPS protocol" MUST provide support for information exchange to realize the "state control interface" and "in-band signaling channel" as defined in [CUPS].

```
               +--------------------------------------+
               | +--------+ +-----+  +-----+  +-----+ |
               | | AAA    | |PCRF |  | OCS |  | OSS | |
               | | Server | +-----+  +-----+  +-----+ |
               | +--------+                           |
               +----------------+---------------------+
                                |
                                |
    "CUPS BNG"                  |
   +----------------------------+------------------------------------+
   |   CP                                                            |
   |   +--------------------------+--------------------------------+ |
   |   | +-----------+ +------------------+ +--------+ +---------+ | |
   |   | | Address   | | PPPoE, DHCPv4/v6 | | RADIUS | | S11/N11 | | |
   |   | | Pool Mmmt | | IPv6 RS/RA,      | | CLIENT | +---------+ | |
   |   | +-----------+ | L2TP LAC         | +--------+             | |
   |   |               +------------------+  +----+  +----+        | |
   |   |                                     | Gx |  | Gy |        | |
   |   |                                     +----+  +----+        | |
   |   +-----------------------------------------------------------+ |
   |          |                  |                   |               |
   |          | Management       |In-band            | State         |
   |          | Interface        |Signaling          | Control       |
   |          |                  |Channel            | Interface     |
   |          |                  |                   |               |
   |  --------+--+------------------+--+----------------+---+------- |
   |          |                        |                    |        |
   |    UP    |               UP       |           UP       |        |
   |    +-----+---------+    +---------+-----+    +---------+-----+  |
   |    | Local CP      |    | Local CP      |    | Local CP      |  |
   |    | Routing, MPLS |    | Routing, MPLS |    | Routing, MPLS |  |
   |    | IGMP, BFD     |    | IGMP, BFD     |    | IGMP, BFD     |  |
   |    +---------------+    +---------------+    +---------------+  |
   |    | Forwarding    |    | Forwarding    |    | Forwarding    |  |
   |    | Traffic Mgmt  |    | Traffic Mgmt  |    | Traffic Mgmt  |  |
   |    +---------------+    +---------------+    +---------------+  |
   |                                                                 |
   +-----------------------------------------------------------------+
```

CUPS BNG System

2.1. State Control Interface Requirements

- "CUPS protocol" MUST support convergence on BNG, where the CPEs terminating connections on the BNG can have fixed-access (e.g. xDSL/PON/Ethernet), fixed-wireless access (LTE/5G) or hybrid-access (i.e. combined fixed and wireless access).

- "CUPS protocol" MUST support messages and information exchange for node level management. There needs to exist a concept of association between CP and UP. When the CP or UP comes online it should setup an association with the configured or discovered peers via a message exchange. In association setup, the nodes should be able to exchange supported capabilities, version of software, load/overload information, and resource information. Also, any node-wide parameters can be exchanged during association setup.

- "CUPS protocol" MUST allow either node to update the association to report changed feature capabilities, overload condition, resource exhaustion or any other node-wide parameters.

- "CUPS protocol" MUST provide support for UP to request a graceful association release from the CP.

- "CUPS protocol" MUST support periodic node-level heartbeat exchange between CP and UP to detect if the peer is reachable and active.

- "CUPS protocol" MUST support exchange of messages and information elements (IEs) between CP and UP for session level state management on the UP.
  A subscriber session is a single IP connection, such as an IPoE or PPPoE session. A CPE can have multiple sessions, if multiple IP connections are required (e.g. one per service, or one per device behind the CPE). The session level state on the UP, managed from the CP includes:

  - Data-plane state for forwarding data traffic from subscriber sessions in upstream direction (access to network), and downstream direction (network to access).

  - Forwarding state related to in-band control plane messages (such as messages for DHCP, PPPoE, SLAAC) that are forwarded

from CPE to CP via the UP (in upstream direction), and from CP to CPE via the UP (in downstream direction).

- In addition to the basic forwarding state, the "CUPS protocol" MUST support messages and information elements (IEs) for CP to associate, update and disassociate other data-plane related state with the session e.g. state related to:
  - Filtering
  - SLA management
  - Statistics collection
  - Credit control (usage monitoring and reporting)
  - Traffic mirroring for legal intercept
  - NAT
  - Application (L4-L7) aware policies

- Depending on the type of access and the network between access-nodes and the BNG, the subscriber traffic from the CPEs can be encapsulated and transported over an L2 connection or over an L3 tunnel. Common scenarios for fixed access include Ethernet (q-in-q,.1q), L2oGRE, L2TPv3, VxLAN, and MPLS PW. For fixed-wireless the access is over a GTP tunnel (as defined in [CUPS]). The tunnel transport for L3 tunneled subscriber traffic can IPv4 or IPv6. The subscriber traffic itself can be IPv4, IPv6 or PPPoE. In case of PPPoE, the BNG can terminate PPPoE or tunnel it over L2TP to another gateway. The data-plane on the BNG decapsulates the upstream (access->network) traffic and routes it towards the network in appropriate routing-context, and optionally perform NAT before routing. It determines the subscriber for downstream (network->access) IP traffic, encapsulates it appropriately before forwarding towards the access. In addition, it does traffic-management and SLA management, maintains traffic statistics and optionally monitors and reports usage. The "CUPS protocol" MUST be able to carry state from CP to UP for IPv4, IPv6 and PPPoE sessions, for various flavors of transport connections mentioned above.

- Given the variety of access types on the CPE and type of transport networks between access-nodes and BNG (as outlined above) , the "CUPS protocol" MUST specify forwarding state information for the subscriber sessions, for both data and in-band control, as flexible packet matching rules and set of actions related to forwarding and traffic management, rather than just fixed-format lookup tables understood by particular UP implementation. Using the flexible match rules and actions conveyed in the "CUPS protocol" IEs, the UP should unambiguously be able to derive

various lookup tables and processing in the forwarding path to forward traffic to and from the CPE. The basic forwarding state in upstream direction (i.e. access to network) and downstream direction (i.e. network to access) fundamentally consists of session identification and one or more actions. Following shows a logical representation of a directive from CP to UP to install basic forwarding state on the UP for fixed L2 access (i.e. access from DSLAM or OLTs over Ethernet).

- o Direction Upstream - Access to Network:
  - . Subscriber-session identification: Port/VLAN-tag(s) + subscriber-MAC + Session IP address + PPPoE Session-ID
  - . Action: remove encapsulation (i.e. Ethernet and PPPoE/PPP headers), apply policer, do IP FIB lookup, forward to network.

- o Direction Downstream - Network to Access:
  - . Subscriber-session identification: IP address
  - . Action: apply subscriber-shaper, build encapsulation using (PPPoE session-id and Port/VLAN-tag(s)+ subscriber-MAC), forward to access.

Examples of actions and processing related to forwarding and traffic management include encapsulation/decapsulation, table lookups, drop, forward, mirror, count, redirect, police, classify, queue, shape etc.

. In addition to packet-matching rules and actions to setup data-path on the UP, the "CUPS protocol" MUST allow CP to specify subscriber routing and IP interface related information. This includes the following:

- o Aggregate IPv4 subnets and IPv6 prefixes that are used for assigning addresses or prefixes (e.g. IPv6 delegated-prefix) to subscribers on a UP. These are announced in routing by the UP to draw downstream traffic.
- o UE's IP address and subnet mask.
- o Default gateway IP address within the subscriber subnets. This is used to draw upstream traffic from the CPEs and the UP is required to respond to ICMP requests for this address from the CPEs.
- o Subnets for network behind a CPE (also known as framed-routes).

- The "CUPS protocol" MUST provide support for CP to specify session level HQOS related information to the UP. A common QOS hierarchy on BNG consists of at least a QoS layer per access-node, and per CPE. "CUPS protocol" MUST provide support for CP to specify QoS parameters (e.g. rates, queues, markings) and the QoS hierarchy to which the CPE belongs, to the UP. The CP may choose to signal this via a QoS policy that is locally pre-configured on the UP. "CUPS protocol" MUST provide support for CP to specify HQOS-policy that the session is associated with.

- "CUPS protocol" MUST support asynchronous session level event notifications from UP to CP. Session level asynchronous notifications include:

  - Periodic usage-reports
  - Threshold based usage-reports
  - Inactivity timeout
  - Subscriber unreachability detection

- "CUPS protocol" MUST support asynchronous node level event notifications from UP to CP. Example includes switchover notification in case ports or UP failures when node level redundancy is enabled.

2.2. Extensibility

- "CUPS protocol" MUST support exchange of software version and feature capabilities when a node level association is setup between a CP and UP.

- "CUPS protocol" MUST encode information in messages as TLVs.

- "CUPS protocol" MUST allow extension to defined Information Elements (IEs) i.e. it MUST allow adding new information to existing IEs while maintaining backwards compatibility.

- "CUPS protocol" MUST allow addition of new IEs exchanged in protocol messages.

- "CUPS protocol" MUST support vendor specific IEs (modelled as TLVs) by carving out TLV space for vendor specific extensions.

- "CUPS protocol" processing on UP MUST support graceful handling when an unknown TLV is received. The UP MUST ignore unknown TLV and continue with normal message processing. This ensures the CP MAY send non-mandatory TLVs to the UP. However, CP MUST only send mandatory TLVs if it knows the UP will accept it (based on local configuration or based on capability exchange during association setup). A TLV is considered mandatory if session state cannot be installed or updated without it.

2.3. Scalability and Performance

- A single CP VNF can control multiple UP nodes. Each UP can support its maximum scale of subscriber sessions as allowed by its data-plane. External control plane running as a VNF can horizontally scale-out as needed with the growth in CUPS system-wide subscriber scale. In typical deployments CP may be centralized whereas the UPs may be distributed, with multiple L2 or L3 hops between CP and UPs. There are scenarios where a large number of sessions may be getting created or deleted close in time via "CUPS protocol". It is important that latency to bring subscribers online is minimized. The transport protocol chosen for "CUPS protocol" MUST NOT suffer from head-of-line (HOL) blocking where transport of messages related to one subscriber can be adversely impacted by messages being exchanged for other subscribers.

- "CUPS protocol" MUST limit chattiness by minimizing number of messages required to create fully functional subscriber on the UP with complete forwarding, traffic management, HQOS, and routing state. Ideally, a single request/response message exchange between CP and UP should be able to create subscriber with all the required state in the data-plane. The "CUPS protocol" message that creates the subscriber session MUST therefore be able to signal IEs for all the required subscriber state.

- To further reduce latency the protocol MUST be binary encoded.

- "CUPS protocol" MUST allow dynamic scale-out for control plane VNF with the growth in subscriber scale of the CUPS system, as more UPs are added to the CUPS system or more ports are enabled on a UP in a CUPS system.

- The "CUPS Protocol" MUST allow mechanism to provide balancing of processing load amongst compute resources of control-plane VNF that supports dynamic scale-out.

- "CUPS protocol" SHOULD support signaling of overload state and optionally overload mitigation parameters from UP to CP, when UP determines the incoming signaling from CP is exceeding (or about to exceed) its nominal processing capacity. Overload mitigation can include a temporary message throttling on CP towards UP. Mitigation parameters can include message rate and validity time for the specified rate.

2.4. Transport Protocol

- As mentioned in section 2.3, the transport protocol used for "CUPS protocol" MUST NOT suffer from HOL blocking. Therefore, TCP is not an option for the transport protocol.

- Ideally, the transport protocol SHOULD preserve message boundary with datagram semantics and should be available or easily implementable on any simple forwarding devices. Therefore, UDP is the preferred option.

- "CUPS protocol" MUST therefore support reliability and ordering for exchanged messages. The reliability and ordering can be based on request/response with message sequencing and re-transmissions.

2.5. In-band Control Channel Requirements

- "CUPS protocol" MUST support setting up of control channel between UP and CP for transporting in-band control messages (e.g. DHCPv4/v6 and PPPoE) received on the UP (from CPEs) to the CP, and for return messages sent from CP to the UP (destined to CPEs).

- There can be a L3 network between CP and UPs. Therefore, L3 tunneling is required between CP and UP to carry messages for in-band control plane protocols. "CUPS protocol" MUST support exchange of tunnel identifiers between CP and UP.

- Because L2 access setup is in-band, control plane messages will arrive on the UP before any per-session state is learned. Therefore, "CUPS protocol" MUST support messages and information exchange to install forwarding state related to in-band control plane messages that do not match any existing subscriber session. These messages should be forwarded to the CP over a common default control channel.

- The in-band control channel setup by "CUPS protocol" MUST have support for UP to pass access-circuit identifier over which the signaling messages are received from the CPEs. Based on type of access, access-circuit identifier can include port/VLAN tags or tunnel identifiers which includes tunnel endpoint IPs and de-multiplexers such as GTP TEID, MPLS labels, L2TP tunnel-id etc. "CUPS protocol" MUST support setting up logically separate control channels for in-band control messages per access-circuit.

- In case of fixed-access CPEs with Ethernet based network between access-nodes and BNG, the control messages are received in Ethernet frames. The Ethernet frame carrying the control messages received on UP MUST be carried over the control channel to the CP, as outlined in [CUPS]. In case of fixed-wireless access, control messages (e.g. DHCPv4 and DHCPv6) are received on the UP over GTP-u tunnel from the RAN. The GTP-u tunnel directly carries IP payload. Therefore, control channel setup via "CUPS protocol" MUST support transporting both Ethernet and IP payloads.

- "CUPS protocol" MUST provide support for CP to specify the control protocols that should be forwarded by the UP over in-band control channel to the CP.

- The "CUPS protocol" SHOULD have support for CP to specify rate-limits for specific control protocols and optionally specific messages within a control protocol, that the UP should enforce.

- The "CUPS protocol" SHOULD provide support for CP to direct the UP to drop certain control messages received on a particular access-circuit.

- The "CUPS protocol" SHOULD provide support for CP to prioritize reception of certain control messages over others.

2.6. Resiliency

- "CUPS protocol" MUST allow support for both 1:1 (hot standby) and N:M (warm standby) UP node level redundancy.

- "CUPS protocol" MUST provide support for CP to specify the "redundancy domain" that a subscriber session is associated with during session level state creation on the UP. The "redundancy domain" is set of resources that share fate with respect to switchover on failure, e.g. a set of VLANs on a port, or a set of ports on a UP, or entire UP. "CUPS protocol" MUST also provide support for CP to provide relevant parameters to UP about the "redundancy domains". The UPs can then locally preform failure detection and switchover for the redundancy domains.

- The "CUPS protocol" MUST provide support for UP to notify the CP about switchover event. This notification must be on the granularity of "redundancy domain" on a UP.

- For warm standby redundancy, "CUPS protocol" MUST provide support for CP to create session level state on the backup UP node(s) for all subscribers associated with the impacted "redundancy domain".

- "CUPS protocol" MUST support in-service software upgrade (ISSU) on UPs. The protocol MUST provide support for UP to notify CP when it is completed ISSU to the new software release.

2.7. Security

"CUPS protocol" MUST be compatible with proven security mechanisms such as IPSEC or DTLS to satisfy following security requirements:

- Data-integrity and confidentiality MUST be ensured for the information exchanged via "CUPS protocol".

- Protection against man-in-the-middle attacks MUST be provided.

- Anti-replay protection MUST be provided.

3. "CUPS protocol" candidate

3GPP has defined PFCP (Packet Forwarding Control Protocol) in [TS29244] as the interface between CP and UP for LTE gateways. This protocol is suited for large scale state management between CP and UP and can be extended for BNG providing converged access. The protocol provides a good base for satisfying the requirements outlined in this draft for BNG "CUPS protocol". Following are some of the key attributes of this protocol/

- It supports management of forwarding and QOS enforcement state on the UP from CP.

- It also supports usage reporting from UP to CP.

- It is over UDP transport and doesn't suffer from any HOL blocking.

- It provides reliable operation based on request/response with message sequencing and retransmissions.

- It provides support for graceful handling of overload on UP.

- The protocol is extensible and allows addition of new IEs.

- For fixed access BNG, the protocol requires simple extensions in the form of additional IEs. The required extensions are mainly due to fact that typically a fixed access BNG requires tighter control over L2 behavior and manages access and subscriber using L2 identifiers (such as VLANs and MAC addresses), whereas mobile access works in terms of L3, either routed or tunneled.

- [TS29244] also describes an in-band signaling channel based on GTP-u tunnel between CP and UP. GTP-u (GPRS Tunneling protocol User Plane) is defined in 3GPP [TS29281] and defines a tunneling protocol which carries IP payloads. The protocol runs over a UDP/IP stack and uses UDP port number 2152. Data within a tunnel can be multiplexed based on Tunnel Endpoint Identifiers (TEIDs). The protocol supports optional sequence numbers. The protocol supports extension headers to allow development of new features. GTP-u tunnels are signaled between CP and UP, and it is possible to associate filters to forward or block certain control packets from UP to CP. The payload type carried by GTP-u can be extended to Ethernet (via payload type in extension header). The tunnel encapsulation can also be extended by introducing an additional NSH (network services header) to carry any required meta-data.

4. Security Considerations

For security between CP and UP, Network Domain Security (NDS) as defined in [TS33210] can be considered. As per NDS, the network can be split into security domains. Communication within a single security domain is considered secure, and protocols can operate without any additional security. When communication has to cross security domains, then IPSEC can be used.

5. Management Interface Requirements

- The CP MUST provide a single point for management of "CUPS BNG" system to the operator.

- Management interface for the CUPS system MUST provide support for both configuration of UPs, and state retrieval. The interface MUST minimally support BNG specific configuration and state.

- Management interface SHOULD support transactional configuration from CP to UPs, based on a well-defined data schema. Transactional configuration may be achieved by editing a candidate configuration on the UP which is subsequently activated (commit) or by providing the whole transaction in a

single command. In case UP data-stores are used, it MUST be possible for the CP to lock a data-store for exclusive access.

- The management interface SHOULD support transaction confirmation, where an unconfirmed transaction gets reverted automatically after a timeout even if the transaction succeeded. This is to avoid configuration errors where a valid configuration breaks communication between UP and CP, requiring on-site intervention.

- The management interface SHOULD support state retrieval based on a well-defined data schema. This includes retrieval for any state that is not signaled via the state control interface.

- The management interface SHOULD support unsolicited signaling of state changes (events) from UP to CP i.e. SHOULD provide telemetry for events. Even while state changes are sent unsolicited, the CP SHOULD be able to subscribe to a specific subset of state it is interested in.

- The management interface MUST provide security through an existing mechanism such as (D)TLS or IPSEC to guarantee confidentiality and authenticity and protect against replay and man in the middle attacks.

6. IANA Considerations

None.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[CUPS] Wadhwa, S. et al., "Architecture for control and user plane separation on BNG, July 2019. https://datatracker.ietf.org/doc/draft-wadhwa-rtgwg-bng-cups/

[TS29244] 3GPP, "Interface between the Control Plane and the User Plane Nodes", TS 29.244 15.2.0, June 2018, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3111.

[TS29281] 3GPP, "General Packet Radio System (GPRS) Tunneling Protocol User Plane (GTPv1-U)", TS 29.281 15.3.0, June 2018, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=1699.

[TS33210] 3GPP, "Network Domain Security (NDS); IP network layer security", TS 33.210 15.0.0, June 2018, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2279.

7.2. Informative References

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, https://www.rfc-editor.org/info/rfc2131.

[RFC2516] Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, DOI 10.17487/RFC2516, February 1999, https://www.rfc-editor.org/info/rfc2516.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, https://www.rfc-editor.org/info/rfc3315.

Authors' Addresses

Sanjay Wadhwa
Nokia
777 East Middlefield Road
Mountain View
USA

Email: Sanjay.wadhwa@nokia.com

Killian De Smedt
Nokia
Copernicuslaan 50
Antwerp
Belgium

Email: Killian.de_smedt@nokia.com

Praveen Muley
Nokia
805. E. Middle Field Rd.
Mountain View, CA, 94043
USA

Email: praveen.muley@nokia.com

Rajesh Shinde
Reliance Jio Infocomm Ltd.
Reliance Corporate Park
Thane Belapur Road, Ghansoli
Navi Mumbai 400710
India

Email: Rajesh.A.Shinde@ril.com

Jonathan Newton
Vodafone
Waterside House
Bracknell
United Kingdom

Email: jonathan.newton@vodafone.com

Ryan Hoffman
TELUS
1525 10th Ave SW
Calgary, Alberta
Canada

Email: ryan.hoffman@telus.com

Subrat Pani
Juniper Networks
10 Technology Park Dr.
Westford, MA
USA

Email: spani@juniper.net