JUNIPER NETWORKS

Network Configuration Example

Deploying Scalable Services on an MX Series Router Acting as a Broadband Network Gateway

Published: 2014-01-10

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Network Configuration Example Deploying Scalable Services on an MX Series Router Acting as a Broadband Network Gateway
NCE0062

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

This document provides information about scalable services available on your Juniper Networks® MX Series 3D Universal Edge Router. Scalable services help you reduce operational and capital overhead. This document explains multiple services that run on the MX Series router, such as PPPoE subscribers, carrier grade NAT (CGN) with dual-stack lite (DS-Lite) subscribers, and dynamic application awareness with deep packet inspection (DPI).

Scalable Services on an MX Series Router Overview

Service providers are increasingly evaluating products to offer their customers value-added services such as network-based security, carrier grade NAT (CGN), and deep packet inspection (DPI). With MX Series 3D Universal Edge Routers, service providers can offer integrated value-added services for their subscriber base beyond basic Broadband Network Gateway functions in traditional deployments. *Example: Deploying Value-Added Subscriber Services with MX Series Routers* covers the versatile Broadband Network Gateway functionality on the MX Series router. The example does not test the MX Series router to its limits, but it describes multiple services such as Point-to-Point Protocol over Ethernet (PPPoE) subscribers, CGN with dual-stack lite (DS-Lite) subscribers, and dynamic application awareness with DPI deployed on a single router. Service providers benefit from the MX Series routers' versatile architecture, which enables value-added services on the Broadband Network Gateway router, reducing the need for external appliances and realizing savings in operational expenses and capital expenses. MX Series routers deliver large-scale performance using the Modular Port Concentrator (MPC) and the MultiService-Dense Port Concentrator (MS-DPC).

In residential broadband networks, triple-play networks provide residential voice and Internet data services that deliver an experience based on a converged IP infrastructure. New subscribers must be provisioned on a daily basis, while existing subscribers can make changes to their service subscriptions. There is a significant amount of subscriber management activity on a daily basis. Subscribers are provisioned with PPPoE or Dynamic Host Configuration Protocol (DHCP) models. A Broadband Network Gateway solution must support all the aspects of subscriber configuration and provisioning in a simple and scalable manner with support for automation and minimal manual configuration. Subscriber characteristics are defined based on service subscription and network resources such as bandwidth and quality of service (QoS) and are provisioned based on the service type.

Related Documentation

- Use Case for Multiple Services on an MX Series Router on page 1
- Example: Deploying Value-Added Subscriber Services with MX Series Routers on page 2

Use Case for Multiple Services on an MX Series Router

Network operators are adding more revenue-generating services by providing dynamic application awareness and provisioning network resources based on application type.

The Juniper Networks solution supports provisioning of the appropriate enforcement functions on the forwarding plane in real time.

Enforcement functions include:

- Rate limiting traffic
- Classifying traffic (DiffServ code point [DSCP] mark for class-of-service [CoS] handling)
- Connection closing, blocking specific application traffic

Dynamic application awareness supports intrusion prevention and tiered service-based billing.

IPv4 address depletion is a reality, and providers are evaluating next-generation networks addressing needs. Service providers are looking for solutions to address IPv4 address exhaustion and ways to easily transition to IPv6 so they can add new subscribers and ensure steady business growth.

MX Series routers are built to deliver 3D scale for bandwidth, subscribers, and services. The combination of a scalable Junos® operating system (Junos OS), the flexibility and programmability of the Junos Trio chipset, and support for advanced security, firewall, and CGN features on the MS-DPC blade together offer an "all in one box" solution. Open Junos SDK service providers can also build custom applications and can differentiate your service offerings.

Related Documentation

- Scalable Services on an MX Series Router Overview on page 1
- Example: Deploying Value-Added Subscriber Services with MX Series Routers on page 2

Example: Deploying Value-Added Subscriber Services with MX Series Routers

This example shows how to configure a Broadband Network Gateway deployment where the service provider is looking for high-scale subscriber management, support for a carrier grade NAT (CGN) technique such as dual-stack lite (DS-Lite) to overcome IPv4 address depletion challenges, and advanced value-added features such as dynamic application awareness with intrusion prevention. Integrating value-added services onto the Broadband Network Gateway router enables you to eliminate many network interconnect links, which simplifies the network architecture, increasing network utilization and reducing operational and capital overhead.

Requirements

This example uses a Juniper Networks MX480 3D Universal Edge Router as the Broadband Network Gateway. A traffic simulator creates real-world subscriber sessions and stateful traffic on one router.

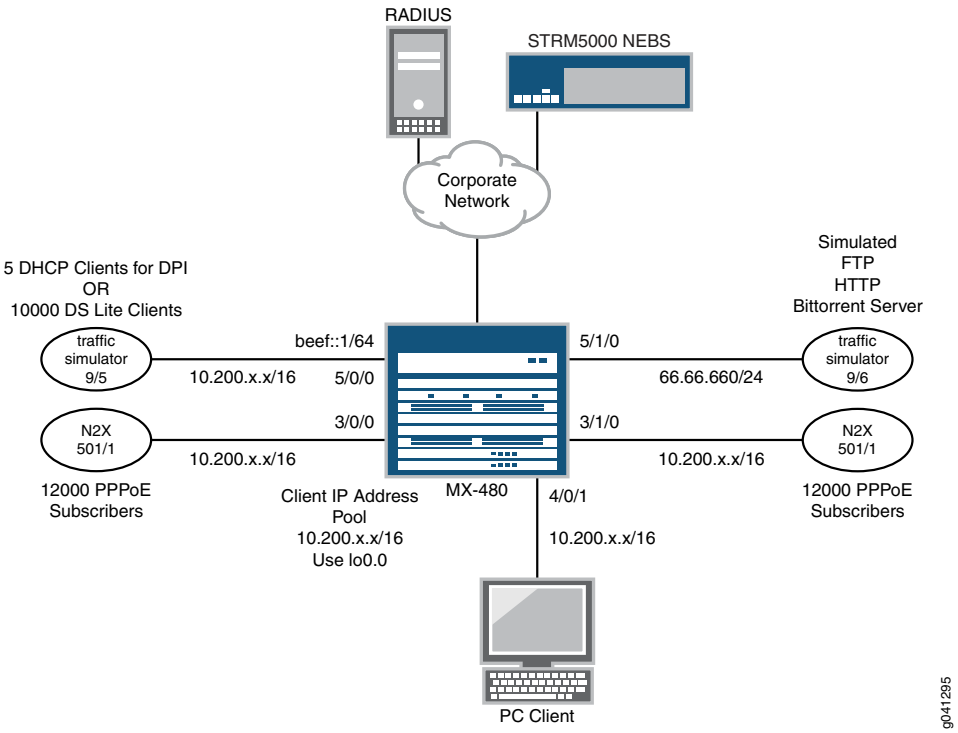
This example uses the following hardware and software components:

- MX480 router running Junos OS 10.4 R3.4
- Three MultiService-Dense Port Concentrators (MS-DPC)
- One Modular Port Concentrator MPC2 Q with one Modular Interface Card (MIC-3D) 4x10GE and one MIC-3D 20x1GE
- Two DPCs

NOTE: This configuration example has been tested using the software release listed and is assumed to work on all later releases.

Overview and Topology

Figure 1: Network Setup to Simulate Customer Requirements



The MX Series router meets your customer requirements of the gateway router for subscriber management, CGN, and additional services of threat management. This network topology contains peripheral test equipment, which simulates subscriber sessions and applications.

- The Security Threat Response Manager (STRM) appliance is used to analyze threat management alerts.

- Testers include a traffic simulator with two 10-Gigabit Ethernet ports for subscriber generation, and a traffic simulator with two 10-Gigabit Ethernet ports for stateful traffic generation.
- A radius server is used to authenticate the Point-to-Point Protocol over Ethernet (PPPoE) and Dynamic Host Configuration Protocol (DHCP) subscribers. Two N2X ports are connected to simulate the PPPoE subscribers. Traffic simulator ports are used to establish the DS-Lite softwires.

Configuration

Provisioning Subscribers with PPPoE

Step-by-Step Procedure

In this example, 24,000 PPPoE subscriber sessions are simulated. Traffic is sent using the simulator. PPP authenticates users before allowing them access to the network, by requiring that they log in to the network using an assigned user ID and password. PPP authentication is tightly integrated with RADIUS. During this authentication phase, the network assigns attributes to individual subscribers by forwarding the login request to a RADIUS server.

To configure conditional installation of prefixes:

1. Configure the PPP options and authentication.

```
[edit]
chassis {
  fpc 1 {
    pic 0 {
      adaptive-services {
        service-package layer-3;
      }
    }
  }
}
```

   The RADIUS server returns information that allows the Broadband Remote Access Server (B-RAS) to determine what to do with the session (filters, multicast enable/disable, bandwidth control, QoS control, policy routing rules, LNS destination, and so on).

2. Configure routing options for the subscriber profiler.

```
[edit]
routing-options {
  access {
    route $junos-framed-route-ip-address-prefix next-hop "$junos-framedroute-
    nexthop";
  }
  access-internal {
    route $junos-subscriber-ip-address {
      qualified-next-hop "$junos-interface-name";
    }
  }
}
```

3. Configure the accounting options.

```
[edit]
accounting-options {
  policy-decision-statistics-profile pdf {
    file lpdf-acct;
    application-aware-access-list-fields {
      address;
      application;
      application-group;
      input-bytes;
      input-interface;
      input-packets;
      mask;
      output-bytes;
      output-packets;
      subscriber-name;
      timestamp;
    }
  }
  file lpdf-acct {
    size 1g;
    files 3;
    transfer-interval 2880;
  }
}
```

4. Configure the RADIUS server details.

```
[edit]
access {
  radius-server {
    100.0.1.2 {
      port 1812;
      secret "$9$6Tgs/tO1IcrlMOBxNbwg4"; ## SECRET-DATA
    }
    100.0.2.2 {
      port 1812;
      secret "$9$DwjqfTQn9Cuf5IEyrvM"; ## SECRET-DATA
    }
  }
}
```

5. Link the **PPPOE-SUBSCRIBER** dynamic profile to the physical interface where subscriber sessions come through.

```
[edit]
Interfaces {
  ge-3/0/0 {
    unit 0 {
      encapsulation ppp-over-ether;
      pppoe-underlying-options {
        dynamic-profile PPPOE-SUBSCRIBER;
      }
    }
  }
  ge-3/1/0 {
    unit 0 {
      encapsulation ppp-over-ether;
```

```
        pppoe-underlying-options {
          dynamic-profile PPPOE-SUBSCRIBER;
        }
      }
    }
  }
```

Configuring DS-Lite Subscribers to Address IPv4 Exhaustion and Transition to IPv6

Step-by-Step Procedure

DS-Lite is a solution that offers both IPv4 and IPv6 connectivity to customers addressed only with an IPv6 prefix. No IPv4 address is assigned to the attachment router. One of this solution's key components is an IPv4-over-IPv6 tunnel, commonly referred to as a softwire. A DS-Lite "Basic Bridging Broadband" (B4) router does not know if the network it is attached to offers DS-Lite service.

A DNS hostname is used to inform the B4 router of the Address Family Transition Router (AFTR) location. Once this information is conveyed, the presence of the configuration indicating the AFTR's location also informs a host to initiate the DS-Lite service and become a software initiator. For more details on DS-Lite and its implementation, go to http://www.juniper.net/ipv6 .

To configure conditional installation of prefixes:

1. Enable the relevant service packages on the MX480 chassis, and configure service options on the MS-DPC where DS-Lite sessions are terminated.

```
[edit]
chassis {
  fpc 1 {
    pic 0 {
      adaptive-services {
        service-package layer-3;
      }
    }
  }
  interfaces {
    sp-1/0/0 {
      services-options ;
    }
  }
}
```

2. Configure the NAT rules.

   With DS-Lite, IPv4 packets are encapsulated in an IPv6 softwire that originates at the B4 router (simulated by a traffic simulator in this case) and terminates on the AFTR (MS-DPC in slot 0 in this case), where they are de-capsulated to IPv4 and address translation is done.

```
[edit]
nat {
  pool p1 {
    address 129.0.0.1/32;
    port {
```

```
        automatic;
      }
      mapping-timeout 86400;
    }
    rule r1 {
      match-direction input;
      term 1 {
        from {
          source-address {
            any-unicast;
          }
        }
        then {
          translated {
            source-pool p1;
            translation-type {
              source dynamic;
            }
          }
        }
      }
    }
  }
```

3. Add the softwire configuration and the associated rule.

```
[edit]
softwire {
  softwire-concentrator {
    ds-lite ds1 {
      softwire-address 1001::1;
      mtu-v6 1460;
    }
  }
  rule r1 {
    match-direction input;
    term t1 {
      then {
        ds-lite ds1;
      }
    }
  }
}
```

4. Configure the service set, link the softwire and the NAT rules to the service, and associate it with the MS-DPC in slot1, the AFTR in this case.

```
[edit]
services {
  service-set sset {
    syslog {
      host local {
        services any;
      }
    }
    softwire-rules r1;
    nat-rules r1;
```

```
        interface-service {
          service-interface sp-1/0/0.0;
        }
      }
    }
```

5. Link the service set to the ingress physical interface (xe-5/0/0) for the DS-Lite traffic from the B4 router (traffic simulator ports 9/5 and 9/6).

   10,000 DS-Lite sessions are simulated from the traffic simulator port, which indicates that 10,000 softwires are up and running.

```
[edit]
interfaces {
  xe-5/0/0 {
    description To-TS-Slot9Port5;
    flexible-vlan-tagging;
    unit 1001 {
      vlan-id 1001;
      family inet6 {
        service {
          input {
            service-set sset;
          }
          output {
            service-set sset;
          }
        }
        address beef::1/64;
      }
    }
  }
}
```

   At this point, there are 24,000 PPPoE subscriber sessions, and 10,000 DS-Lite sessions are on the MX Series router.

Configuring Threat Management

Step-by-Step Procedure

Now that the subscriber sessions are set up, you can enable Dynamic Application Awareness and test the intrusion prevention capability of the router. The Dynamic Application Awareness for the Junos OS set of services adds support for the intrusion detection and prevention (IDP) functionality using deep packet inspection (DPI) technology to Juniper Networks MX Series routers equipped with MS-DPCs.

DPI is configured on the MX Series router using service-sets. IDP depends on application identification services (APPID) for definition and detection of some layer 7 applications.

NOTE: **Before configuring any IDP policy, download the APPID application package.**

To configure threat management:

1. Configure the service package.

```
[edit]
chassis {
    fpc 0 {
        pic 0 {
            adaptive-services {
                service-package {
                    extension-provider {
                        control-cores 1;
                        data-cores 2;
                        data-flow-affinity;
                        object-cache-size 512;
                        package erm-ctrl;
                        package erm-data;
                        syslog {
                            external any;
                        }
                    }
                }
            }
        }
    }
}
interfaces {
    ms-2/0/0 {
        unit 0 {
            family inet;
        }
    }
}
```

2. To configure IDP properties, include statements at the **[edit security idp]** hierarchy level.

In general, configure IDP processes by including the **idp-policyl** statement. Configure the IDP policy and include the recommended multiple match conditions.

```
[edit]
security {
  idp {
    idp-policy idp-policy1 {
      rulebase-ips {
        rule r1 {
          match {
            attacks {
              predefined-attack-groups [ "[Recommended]Critical"
                "[Recommended]Major" "[Recommended]Minor"
                "[Recommended]Info" ];
            }
          }
          then {
            action {
              no-action;
            }
            notification {
              log-attacks;
            }
          }
        }
      }
    }
  }
}
```

3. Configure the application profile.

```
[edit]
services {
  application-identification {
    rule rule1 {
      application-name test2;
      address 1 {
        source {
          ip 10.110.1.1/16;
          port-range {
            tcp 1110-1150;
          }
        }
        destination {
          ip 10.11.1.1/16;
          port-range {
            tcp 111-1100;
          }
        }
        order 1;
      }
    }
    rule-set rs1 {
      rule rule1;
    }
    profile ai_profile1;
```



```
        rule-set rs1;
    }
}
```

4. Define the service set to include the IDP policy, application profiles, and any other application-aware access list (AACL) rules defined.

   This service set is then linked to the MS-DPC, which performs all the threat management processing and forwards any alerts to the STRM appliance.

```
[edit]
services {
    service-set test_sset {
        aacl-rules aacl_rule;
        application-identification-profile ai_profile1;
        idp-profile idp-policy1;
        policy-decision-statistics-profile {
            pdf;
        }
        interface-service {
            service-interface ms-2/0/0.0;
        }
    }
}
```

5. Configure a dynamic profile, and link the service set **test_sset** to the subscriber profile interface.

```
[edit]
dynamic-profiles {
    base_dyn_profile {
        interfaces {
            "$junos-interface-ifd-name" {
                unit "$junos-underlying-interface-unit" {
                    family inet {
                        service {
                            input {
                                service-set test_sset;
                            }
                            output {
                                service-set test_sset;
                            }
                        }
                    }
                    family inet6 {
                        unnumbered-address lo0.0;
                    }
                }
            }
        }
    }
}
```

   The traffic from the DHCP and PPPoE subscribers is detected by the DPI engine, and the information is then sent to the STRM application. STRM appliances are designed to respond to the right threats at the right time through effective analysis of networks, events, and audit log files. STRM appliances can identify environmental

anomalies in the network, an attack path, and the source of a threat. STRM appliances provide network remediation for threat responses across all security products.

Results

The configuration and verification parts of this example have been completed. The following sections are for your reference.

DS-Lite Relevant Configuration

```
chassis {
  fpc 1 {
    pic 0 {
      adaptive-services {
        service-package layer-3;
      }
    }
  }
}
interfaces {
  sp-1/0/0 {
    services-options {
      syslog {
        host local {
          services any;
        }
      }
    }
    unit 0 {
      family inet;
      family inet6;
    }
  }
  xe-5/0/0 {
    description To-TS-Slot9Port5;
    flexible-vlan-tagging;
    unit 1001 {
      vlan-id 1001;
      family inet6 {
        service {
          input {
            service-set sset;
          }
          output {
            service-set sset;
          }
        }
        address beef::1/64;
      }
    }
  }
}
services {
  service-set sset {
    syslog {
      host local {
```

```
            services any;
          }
        }
        softwire-rules r1;
        nat-rules r1;
        interface-service {
          service-interface sp-1/0/0.0;
        }
      }
      softwire {
        softwire-concentrator {
          ds-lite ds1 {
            softwire-address 1001::1;
            mtu-v6 1460;
          }
        }
        rule r1 {
          match-direction input;
          term t1 {
            then {
              ds-lite ds1;
            }
          }
        }
      }
      nat {
        pool p1 {
          address 129.0.0.1/32;
          port {
            automatic;
          }
          mapping-timeout 86400;
        }
        rule r1 {
          match-direction input;
          term 1 {
            from {
              source-address {
                any-unicast;
              }
            }
            then {
              translated {
                source-pool p1;
                translation-type {
                  source dynamic;
                }
              }
            }
          }
        }
      }
    }
```

DPI Relevant Configuration

```
dynamic-profiles {
  base_dyn_profile {
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-underlying-interface-unit" {
          family inet {
            service {
              input {
                service-set test_sset;
              }
              output {
                service-set test_sset;
              }
            }
          }
          family inet6 {
            unnumbered-address lo0.0;
          }
        }
      }
    }
    protocols {
      igmp {
        interface "$junos-interface-name" {
          version 2;
          immediate-leave;
          promiscuous-mode;
        }
      }
    }
  }
  PPPOE-SUBSCRIBER {
    interfaces {
      pp0 {
        unit "$junos-interface-unit" {
          ppp-options {
            pap;
          }
          pppoe-options {
            underlying-interface "$junos-underlying-interface";
            server;
          }
          no-keepalives;
          family inet {
            service {
              input {
                service-set test_sset;
              }
              output {
                service-set test_sset;
              }
            }
            unnumbered-address lo0.0;
          }
        }
      }
```

```
    }
    protocols {
      igmp {
        interface "$junos-interface-name" {
          immediate-leave;
          promiscuous-mode;
        }
      }
    }
    routing-options {
      access {
        route $junos-framed-route-ip-address-prefix next-hop "$junos-framedroute-
        nexthop";
      }
      access-internal {
        route $junos-subscriber-ip-address {
          qualified-next-hop "$junos-interface-name";
        }
      }
    }
  }
}
chassis {
  fpc 2 {
    pic 0 {
      adaptive-services {
        service-package {
          extension-provider {
            control-cores 1;
            data-cores 4;
            object-cache-size 512;
            policy-db-size 64;
            package jservices-appid;
            package jservices-aacl;
            package jservices-llpdf;
            package jservices-idp;
          }
        }
      }
    }
  }
}
interfaces {
  ms-2/0/0 {
    unit 0 {
      family inet;
    }
  }
  ge-4/0/1 {
    unit 0 {
      encapsulation ppp-over-ether;
      pppoe-underlying-options {
        dynamic-profile PPPOE-SUBSCRIBER;
      }
    }
  }
```

```
xe-5/0/0 {
    description To-TS-Slot9Port5;
    flexible-vlan-tagging;
    unit 1 {
        vlan-id 1;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 10.200.0.1;
        }
    }
    unit 2 {
        vlan-id 2;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 10.200.0.1;
        }
    }
    unit 3 {
        vlan-id 3;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 10.200.0.1;
        }
    }
    unit 4 {
        vlan-id 4;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 10.200.0.1;
        }
    }
    unit 5 {
        vlan-id 5;
        family inet {
            unnumbered-address lo0.0 preferred-source-address 10.200.0.1;
        }
    }
}
xe-5/1/0 {
    description To-TS-Slot9Port6;
    flexible-vlan-tagging;
    unit 999 {
        description To-TS-Slot2Port2;
        vlan-id 999;
        family inet {
            address 66.66.66.1/24;
        }
    }
}
accounting-options {
    policy-decision-statistics-profile pdf {
        file lpdf-acct;
        application-aware-access-list-fields {
            address;
            application;
            application-group;
            input-bytes;
            input-interface;
            input-packets;
            mask;
```

```
            output-bytes;
            output-packets;
            subscriber-name;
            timestamp;
          }
        }
        file lpdf-acct {
          size 1g;
          files 3;
          transfer-interval 2880;
        }
      }
    security {
      idp {
        idp-policy idp-policy1 {
          rulebase-ips {
            rule r1 {
              match {
                attacks {
                  predefined-attack-groups [ "[Recommended]Critical"
                  "[Recommended]Major" "[Recommended]Minor" "[Recommended]Info"
                    ];
                }
              }
              then {
                action {
                  no-action;
                }
                notification {
                  log-attacks;
                }
              }
            }
          }
        }
      }
    }
    services {
      application-identification {
        ~
        ~
        ~
        profile ai_profile1;
      }
      service-set test_sset {
        aacl-rules aacl_rule;
        application-identification-profile ai_profile1;
        idp-profile idp-policy1;
        policy-decision-statistics-profile {
          pdf;
        }
        interface-service {
          service-interface ms-2/0/0.0;
        }
      }
    }
```

Related Documentation

- Scalable Services on an MX Series Router Overview on page 1
- Use Case for Multiple Services on an MX Series Router on page 1