

Oracle® SD-WAN

Implementation Guide



Original Publication Date: Nov 1, 2019



Copyright © 2019, 2007 Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. Windows® 7 and Windows® XP are trademarks or registered trademarks of Microsoft Corporation.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

| | |
|--|----|
| About This Document..... | 3 |
| Audience | 3 |
| References | 4 |
| How to Deploy Talari | 5 |
| Example Network | 5 |
| Basic Talari Concepts | 6 |
| WAN Link Configuration | 7 |
| Topology Design Specifics | 8 |
| Configuration Elements | 10 |
| Talari Basic Configuration File Required Information | 10 |
| Talari Basic Configuration | 13 |
| Creating the Connections | 20 |
| Route Configuration | 20 |
| WAN Link Provisioning | 23 |
| Policy Based Routing for the Single Router and Multiple WAN Links | 27 |
| Firewall Rules and NAT | 28 |
| Appendix A - Provisioning | 28 |
| The Concept of Using Shares | 28 |
| Provisioning Groups | 29 |
| Fair Shares | 29 |
| Services | 29 |
| Shares of Group | 29 |
| Dynamic Conduit Provisioning | 30 |

About This Document

The purpose of this guide is to provide the reader with an understanding of how to implement a Talari WAN. This guide covers basic Talari WAN concepts, topology selection, design requirements, and creation of the Talari Configuration File. This guide will also cover how to implement certain Talari features, and the impact of those features on the Talari WAN. The reader of this document is expected to be a network administrator or a network architect.

This document is current as of Talari Adaptive Private Networking (APN) 4.0 GA.

My Oracle Support

My Oracle Support (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
 - For technical issues such as creating a new Service Request (SR), select 1.
 - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click Industries.
3. Click the Oracle Communications link.

Under the SD-WAN header, select a product.

4. Select the Release Number.

A list of the entire documentation set for the selected product and release appears.

5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available:

- *Talari Glossary*
- *Talari Appliance Quick Start Guide*
- *Talari APN New Features Guides* (available for each major and minor release)
- *Talari APN Configuration File Reference* (available for each major and minor release)
- *How to Configure Talari Appliance High Availability*
- *How to Configure Firewalls in a Talari WAN*

How to Deploy Talari

This guide will describe the requirements for implementing Oracle Talari Appliances in an existing network. The first step in the implementation process is to decide where the Talari Appliances will be deployed within the existing infrastructure. This section describes the network topology that will be used for this implementation guide and options for deploying a Talari WAN. The next step is gathering information required for creating a configuration file, then actually creating the configuration file for Talari WAN. Once the Topology is decided upon and the configuration file is created, the user can then deploy their Talari Appliances.

Example Network

This section provides details regarding an incumbent network topology that will be used as an example throughout this guide.

Figure 1 illustrates the incumbent network, which consists of three sites: a corporate data center at New York and two remote sites at London and Hong Kong. In this example, only New York and London will be included in the Talari WAN; Hong Kong will remain a traditional MPLS Intranet site (a non-Talari site). The diagram displays two WAN circuits, an MPLS circuit and an Internet circuit. In the incumbent network, the MPLS circuit provides Intranet connectivity between sites while the Internet circuit provides Internet access as well as a backup VPN service in the event of an MPLS failure. The bandwidth for each circuit is shown in the diagram.

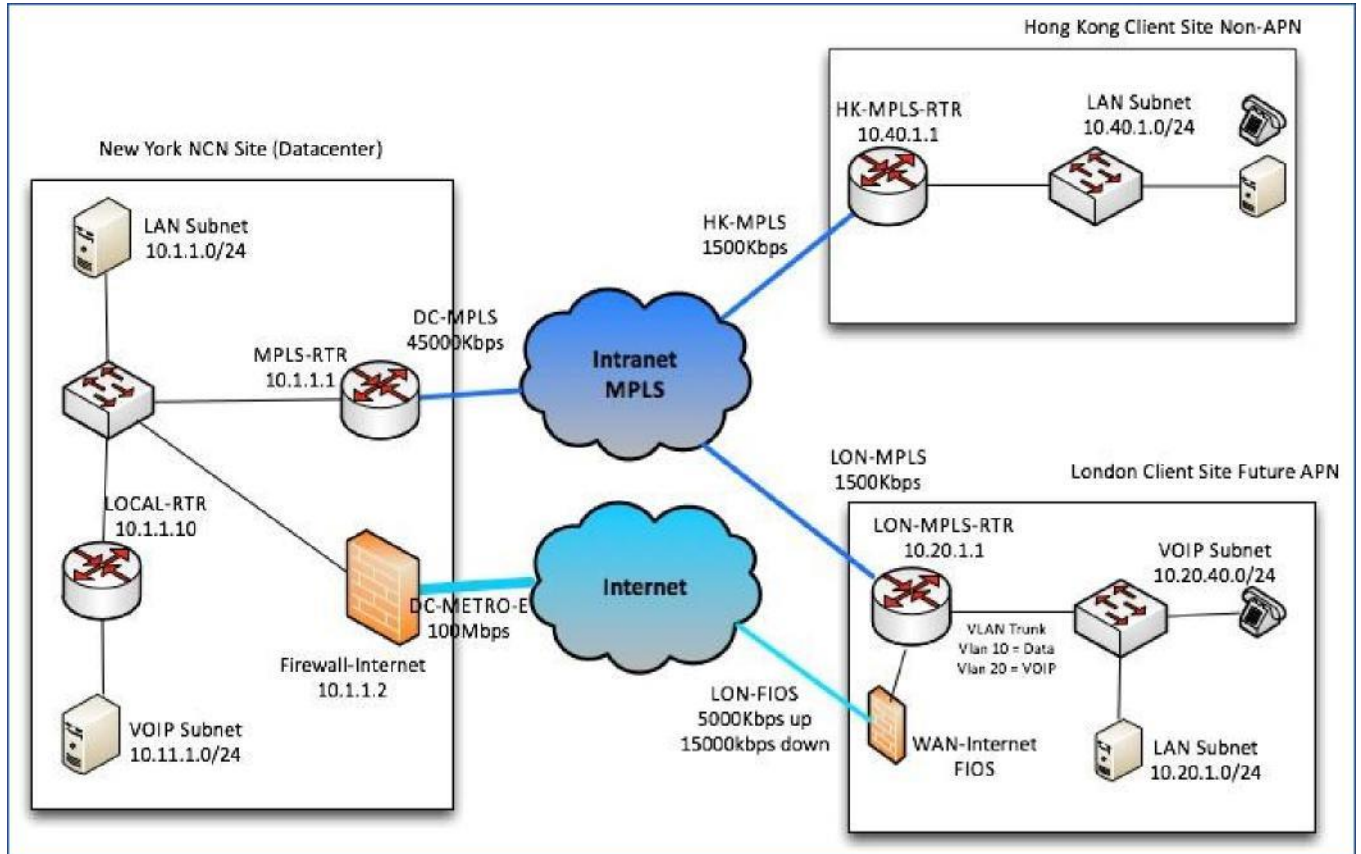


Figure 1 Example Network

Basic Talari Concepts

A **Talari WAN** is comprised of multiple Oracle Talari Appliances, the Conduits between them, and other Talari Services. Below is a listing of major Talari concepts. See the *Talari Glossary* for an explanation of additional concepts that may be encountered throughout this guide.

- **Network Control Node (NCN):** A Talari Appliance that acts as the master controller of the Talari WAN and the central point of administration for the Client Nodes. The NCN's primary purpose is to establish and utilize Conduits with one or more Client Nodes located across the network for Enterprise Site-to-Site communications.
- **Client Node (Client):** A Talari Appliance that is located across the Talari WAN from the Network Control Node (NCN). Although an NCN may potentially have multiple Clients, each Client has only one NCN.
- **WAN Link:** The general term for a Talari Appliance's connection to a WAN. WAN Links are typically connected to router ports. Some examples of WAN Links are T1, Cable, DSL, or Frame Relay. Each WAN Link is assigned a Talari Virtual IP address (VIP).
- **WAN Path (Path):** A logical, unidirectional connection between two WAN Links (i.e. two Talari VIPs). By default, Talari encapsulated frames use the Talari Reliable Protocol (TRP). Talari Path traffic is encapsulated in UDP using a default port of 2156.

- **Conduit Service (Conduit):** A service that is a logical combination of one or more Paths. This is the typical service for enterprise, Site-to-Site Intranet traffic using the full value of the Talari WAN. Depending on the configuration, traffic is managed across multiple WAN Links to create an end-to-end tunnel.
- **Intranet Service:** A service used for any Enterprise Intranet traffic that is not defined for transmission across a Conduit. Traffic of this type is not encapsulated. The Talari WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Under certain conditions, and if configured for Intranet Fallback on the Conduit, traffic that ordinarily travels via a Conduit may instead be treated as Intranet traffic to maintain network reliability.
- **Internet Service:** A service used for traffic between a Talari Site and sites on the public Internet. Traffic of this type is not encapsulated. The Talari WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion.
- **Passthrough Service:** Traffic directed to the Passthrough service includes broadcasts, Address Resolution Protocol (ARPs), other non-IPv4 traffic, and traffic on the Talari Appliance's local subnet (e.g., specifically configured subnets or rules applied by the network administrator). The Talari Appliance does not delay, shape, or modify this traffic. Because the Passthrough Service does not hinder this traffic, network administrators must ensure that it does not consume substantial resources on the WAN Link that the Talari Appliance is configured to use for other services.

WAN Link Configuration

Figure 1 includes information that will be required for the Talari configuration file. Since the MPLS circuit is a shared circuit between existing sites, we need to define what portion of the MPLS circuit is available for Conduit traffic at each site. In addition, New York and London have Internet WAN Links that will be used to support both Conduit traffic and Internet traffic. Internet WAN Links are typically used for VPN services or Internet connectivity. Talari allows these WAN Links to be used for Conduit services and then a percentage of the WAN Link can be provisioned for Internet access, if required.

For each WAN Link, the following information must be defined in the Talari configuration:

- WAN Link Name
- WAN Ingress (Upload) Bandwidth (Kbps)
- WAN Egress (Upload) Bandwidth (Kbps)
- Conduit Service Shares (%)
- Intranet Service Shares (%)
- Internet Service Shares (%)

The following tables illustrate how the WAN Links for the example network would be defined. Remember that only New York and London will be included in the Talari WAN; Hong Kong will remain a traditional MPLS Intranet site (a non-Talari site).

| WAN Link Name | WAN Ingress Permitted B/W (Kbps) | WAN Ingress Permitted B/W (Kbps) | Conduit Service Shares | Internet Service Shares | Intranet Service Shares |
|---------------|----------------------------------|----------------------------------|------------------------|-------------------------|-------------------------|
| DC-MPLS | 45000 | 45000 | 30% | N/A | 70% |
| DC-Metro-E | 100000 | 100000 | 50% | 50% | N/A |

Table 1 WAN Link Configuration for New York (Data Center)

| WAN Link Name | WAN Ingress Permitted B/W (Kbps) | WAN Ingress Permitted B/W (Kbps) | Conduit Service Shares | Internet Service Shares | Intranet Service Shares |
|---------------|----------------------------------|----------------------------------|------------------------|-------------------------|-------------------------|
| LON-MPLS | 1500 | 1500 | 70% | N/A | 30% |
| LON-FIOS | 5000 | 15000 | 50% | 50% | N/A |

Table 2 WAN Link Configuration for London

| WAN Link Name | WAN Ingress Permitted B/W (Kbps) | WAN Ingress Permitted B/W (Kbps) | Conduit Service Shares | Internet Service Shares | Intranet Service Shares |
|---------------|----------------------------------|----------------------------------|------------------------|-------------------------|-------------------------|
| HK-MPLS | 1500 | 1500 | N/A | N/A | 100% |

Table 3 WAN Link Configuration for Hong Kong

Note: Every WAN Link name in the Talari configuration must be unique. Best practice is to use combine Site name and WAN Link type (e.g. LON-MPLS for “London MPLS WAN Link”).

Bandwidth shares for the various Talari services are enforced when bandwidth is under contention. If there is no contention, all bandwidth is available for any service except for a small portion reserved for Talari control traffic. For more details on bandwidth sharing, see

Appendix A.

In some cases it is necessary to make changes to the Network infrastructure to guarantee the available bandwidth for the Talari Appliance (for example DMZ traffic that the appliance doesn’t see). The user may need to configure Quality of Service (QoS) on the router or firewall to guarantee the permitted rate for the Talari Conduit service.

Topology Design Specifics

Figure 2 shows how Talari Appliance have been deployed at New York and London. The appliances are deployed fully inline (sometimes referred to as overlay topology). This topology allows all user traffic to flow through the appliance. In this topology, the appliance will only place traffic matching a certain criteria into the Conduit. When deploying a Talari Appliance inline, the LAN and WAN ports are not tied to physical ports and can be interchanged, the appliance will determine which port is LAN and which is WAN based on which side the WAN/LAN gateways reside. From a best practice approach, the user should be consistent when the physical deployment is performed. For example, LAN port is consistently addressed as Port

1 and the WAN port is consistently addressed as Port 2. This aids in any potential troubleshooting. In the Datacenter at New York, 2 pairs of fail-to-wire ports are used to create an interface group, in which the Talari Appliance sits between the LAN segment and the WANside MPLS router and firewall.

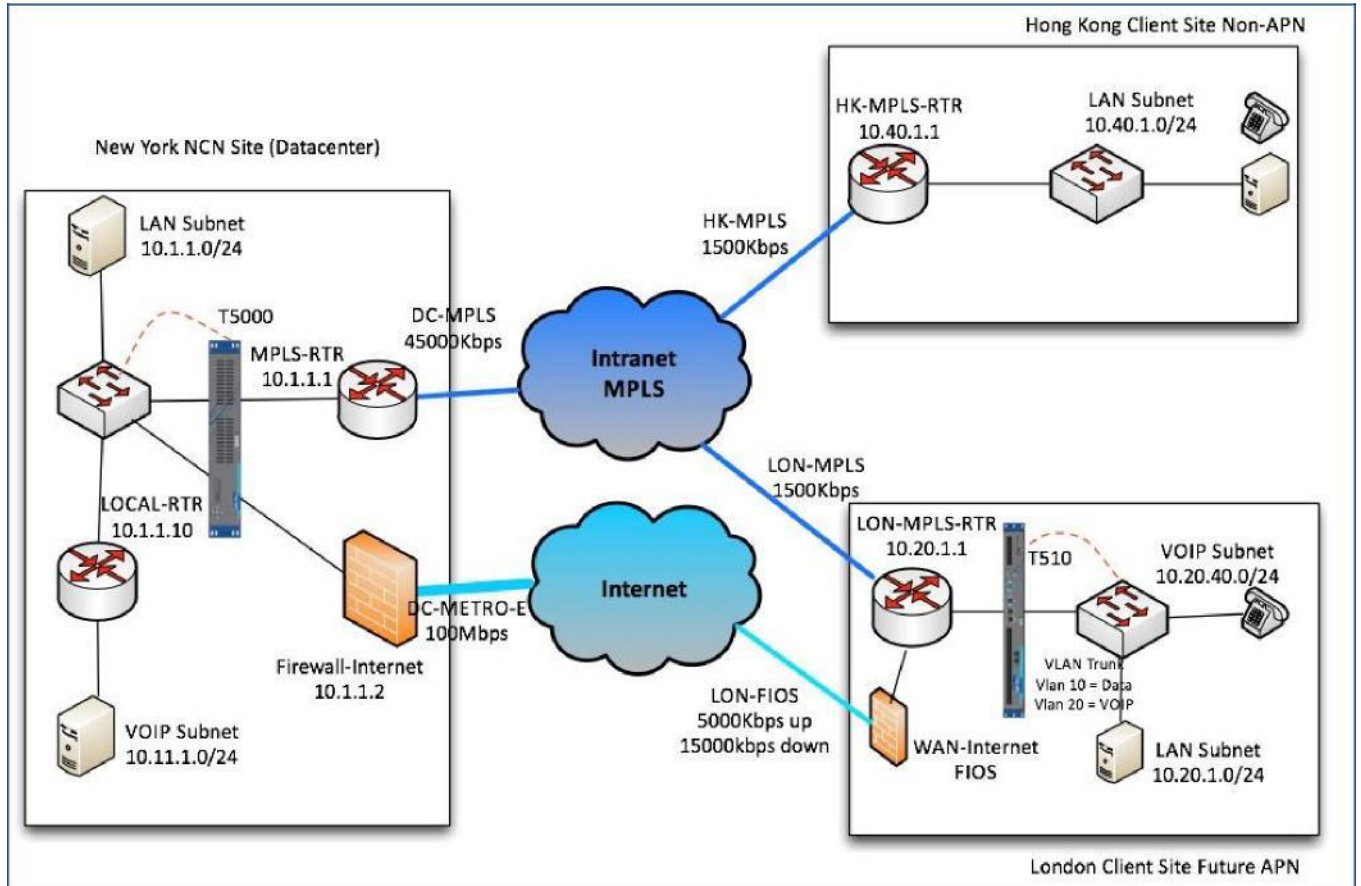


Figure 2 Example Network with Talari Deployed

The inline topology also supports the concept of a bypass pair, which uses the fail-to-wire capability. This capability will allow the Talari Appliance to fail-to-wire (FTW), and pass traffic through a designated port in the event of a power outage or the appliance being disabled. Review the individual appliance hardware guide for platform specifics.

If desired, certain appliances can also support the fail-to-block (FTB) capability. When power is lost to a Talari Appliance configured for FTB the traffic will not pass through the appliance, it will be blocked.

The standard inline design typically includes the management port of the appliance being connected to the LAN segment. As shown in Figure 2 (dotted red connections) the management port of each Talari Appliance is connected to the LAN switch.

Configuration Elements

From the above topology and WAN Link description, we can define specific items that are required to create the configuration file. These include the following:

- Topology (Inline vs. 1-arm)
- Physical Talari Appliance port layout (LAN vs. WAN)
- Management port location on LAN-side
- WAN Link physical speeds and Talari permitted rates
- IP addresses for WAN and LAN gateways
- IP address for management port and WAN Link Virtual IP addresses (VIPs)
- Subnets associated with infrastructure
- WAN Link connecting through gateway or firewall?
- VLAN requirements (optional)

Each Talari Appliance will need to be reachable via its management port to perform the initial configuration. The configuration requirements section provides detail on specific Talari information that is required to establish a basic Talari configuration. The configuration can then be used to establish the Talari Conduits between appliances. As stated earlier, the Talari Conduit consists of logical paths between Talari Appliances. These paths are created by the WAN Link VIP addresses defined in each appliance. The NCN appliance will create a Virtual path on the MPLS WAN Link and separate Virtual path on the Internet WAN Link. These Virtual paths are used to create the Conduit. In addition, traffic for each path must only flow across the defined WAN Link.

Note: All Internet WAN Links can reach other Internet WAN Links and hence paths can be created automatically. When WAN Links are “Private Intranet” they may be able to see other WAN Links of the same mode and service provider. WAN Links of this mode can be added to the same auto-path group so the Conduit paths can be auto-generated. Otherwise the paths can be added manually.

Talari Basic Configuration File Required Information

Information required for creating a basic configuration will include the following for each appliance:

- Management IP address for appliance Talari Model number
- Security key (auto-generated or static)
- Site name
- Appliance Name
- Appliance mode (NCN or client)
- Topology information (fail-to-wire, appliance port configuration, trusted/untrusted)

- VLAN tagging information, if any
- Host/Subnet for Virtual interface (VI)
- Virtual IP address (VIPs) for WAN Links, one IP per WAN Link definition
- Gateway IP address for each defined WAN Link
- Public IP address, if Internet Link (static entry if NCN Site required)
- WAN Link definition – private Intranet (MPLS Link), or public Internet (Internet Link)
- WAN Link physical rates and permitted rates (permitted rate describes rates available for the Talari Conduit)
- Percentage of WAN Link for Conduit, Internet and or Intranet Service

There are some additional configuration items that may be needed to complete the configuration, including:

- Additional routes - if needed, other than the specific Virtual Interface information. By default, only traffic matching the Virtual Interface subnet will be in the Conduit. Users must add additional routes if other subnets are destined for Conduit services. In our diagram above, the inline subnet would be 10.1.1.0/24 at the NCN Site. It is not recommended to add a gateway for the inline subnet unless it has a higher cost than the default value of 5.
- At a Client Site, how WAN Links will be defined will need to be determined. Auto learn or public static IP definition, as well as UDP hole-punching is optional depending on infrastructure.
- Proxy ARP capability, which will be described later in this document.
- Rules and Classes - by default all user traffic is mapped to a default class and rules definitions. The user may define rules and classes once the Conduit is operational to change this default behavior. This requires the user to define the applications that exist and map them to a defined class.
- Application flows (behavior) with or without Talari.

Once this information is collected, the user can create the configuration file using the Talari Configuration Editor available from the NCN or from Talari Aware. The next section provides an explanation of configuration options.

For our example network in [Figure 2](#), we have gathered the following information:

| | |
|----------------|--------------|
| Site Name | New_York |
| Appliance Name | NY_T5000_NCN |

| | |
|------------------------------|--|
| Management IP | 10.1.1.100 |
| Security Key | Auto-generated |
| Model | T5000 |
| Mode | NCN |
| Topology info | Dual inline Fail2wire |
| Virtual Interface IP address | 10.1.1.11/24 10.1.1.12/24 (VIP for the Internet Link) |
| MPLS GW IP address | 10.1.1.1 |
| Internet GW IP address | 10.1.1.2 (public IP=200.231.24.1) |
| Downstream local routes | 10.11.1.0/24 via 10.1.1.10 |
| VLAN Trunks | No |

Table 4 Site Information for New York (Data Center)

| | |
|------------------------------|--|
| Site Name | London |
| Appliance Name | LON_T510 |
| Management IP | 10.20.1.100 |
| Security Key | Auto-generated |
| Model | T510 |
| Mode | Client |
| Topology info | single inline Fail2wire |
| Virtual Interface IP address | 10.20.1.11/24 VLAN 10 (Data) 10.20.1.12/24 (VIP for FIOS Link) 10.20.40.11/24 VLAN 20 (VoIP) |
| MPLS GW IP address | 10.20.1.1 |
| Internet GW IP address | 10.20.1.1 (public IP=auto learn) |
| Downstream local routes | N/A |

VLAN Trunks

Yes – VLAN 10 & VLAN 20

Table 5 Site Information for New York

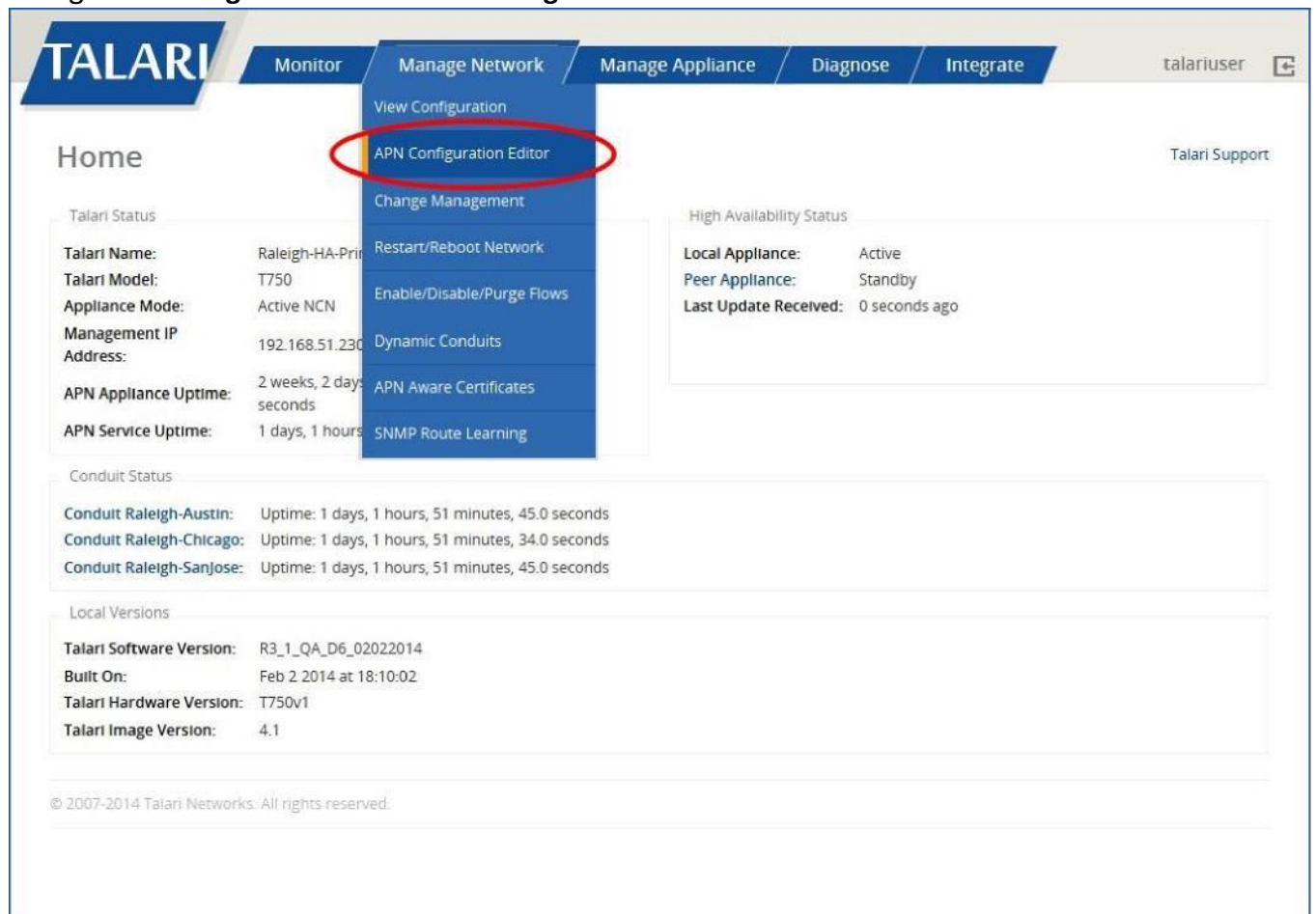
Note: You will need an IP address for each WAN Link you have at each site to be the Virtual_IP (VIP) for each Talari Conduit tunnel. In the case of a firewall that is NAT'd to a public IP you will need to know what the Public IP is at the NCN location. Other Public IPs at Client Sites can be auto learned.

Talari Basic Configuration

The Talari configuration is separated into three sections:

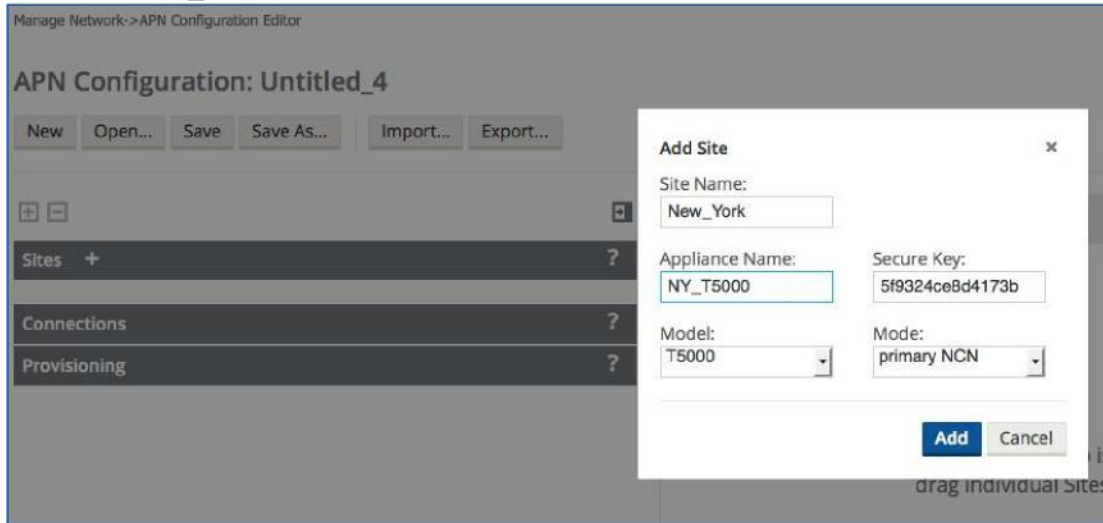
- Site (define the physical information per location)
- Connections (create the connections between the WAN Links at each site)
- Provisioning (define the BW and services for each WAN Link)

To create a configuration, login to the web console of the Network Control Node (NCN), then go to: **Manage Network -> APN Configuration Editor**.



From here we can begin to create the configuration for the entire network. A Talari configuration is holistic meaning the network is managed as one definition and the individual node configurations are derived from this definition. This eliminated a great deal of complexity.

A new configuration can be created and first step is to define all the sites that will have Talari Appliances. Start with the NCN Site (in our example, a T5000 is used as the NCN), in this Case New_York:




Note: Names in Talari Configurations cannot have spaces; use dashes or underscores instead.

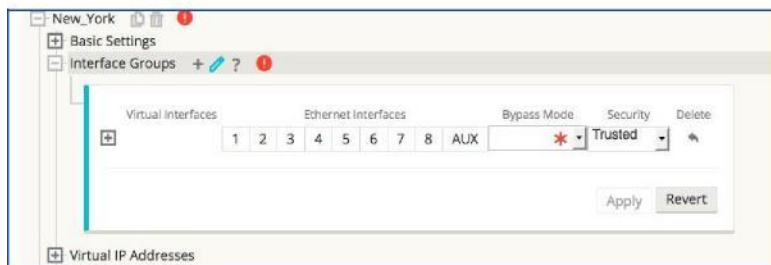
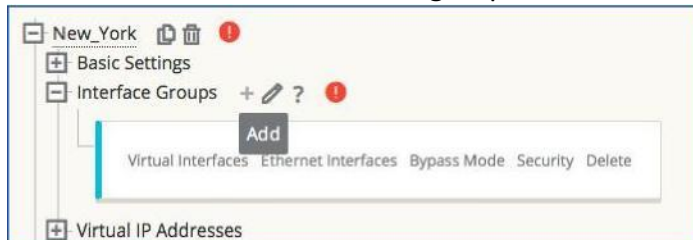
Note: Audit errors highlight the dependencies between certain sections and lead the user to complete the configuration. The configuration tool works from the top to the bottom.


Repeat the step for the London site. Then we can begin to define each site in terms of Interface Groups, Virtual IP addresses and VLANs.



Note: You will notice a network MAP on the right hand side of the configuration tool. You can drag the sites onto the map to represent them graphically. Additionally the map can be moved out of the way by sliding it to the right using the bar in the center.

Now for each site we must configure the Interface groups. This defines the physical ports that we are using and certain behavior of these ports. You will notice the  signs. These show where further configuration is needed. For the New_York Site expand the interface group section, and add a new interface group:

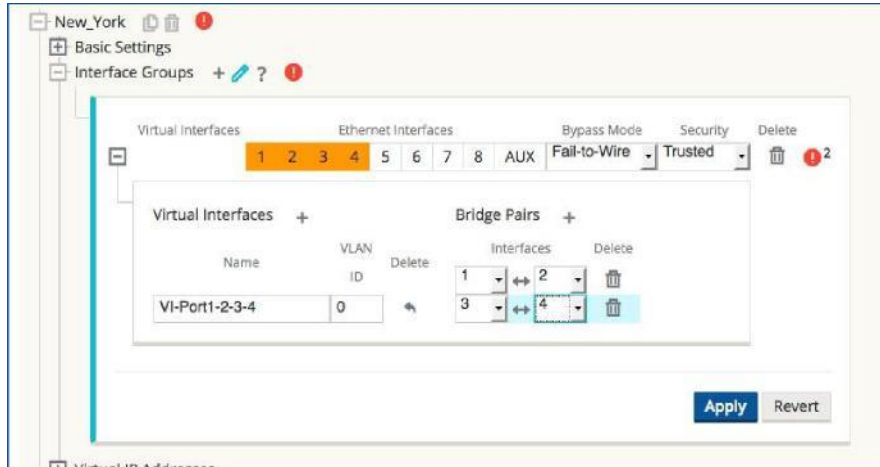


Note: In All cases the + sign allows a new object to be added and the  symbol allows a section to be edited. Revert exits the edit mode. A new section cannot be edited if you are in edit mode. There are tool tips and interactive help sections throughout.

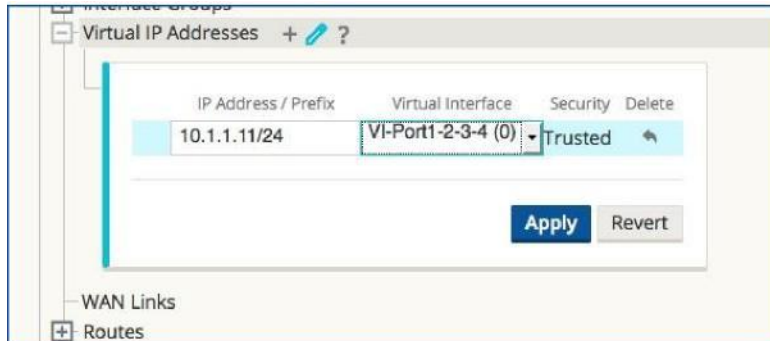
We can now see that we can select which ports will belong to this interface group, what the bypass mode will be and the Security State. In the case of New_York, we are using ports 1, 2, 3 & 4. These are two pairs of fail to wire ports: 1:2 & 3:4. Since the subnet between the MPLS router, Firewall and local core is the same (10.1.1.0/24), we will create a single interface group. If they were different subnets we would create separate interface groups. Not all Ethernet ports on Talari Appliances can be fail-to-wire. Refer to the relevant hardware guide for more information on a specific appliance mode. The security mode can be trusted or untrusted. Untrusted is used when a port is connecting directly to the Internet, and is not behind a firewall.

Once the ports, bypass mode and security mode have been selected we can also create the VLAN configuration and bypass pair associations. Click the + to expand the Virtual Interface box and create other VLANs as needed. In the case of New_York there is no VLAN so we use VLAN_ID=0. Give the Virtual interface a name to identify it in some way. In this case we are using VI-Port-1-2-3-4:

Implementation Guide



The next step is to assign a Virtual IP (VIP) Address to our Virtual Interface (VI). Expand the Virtual IP Addresses section and select add with the + sign:



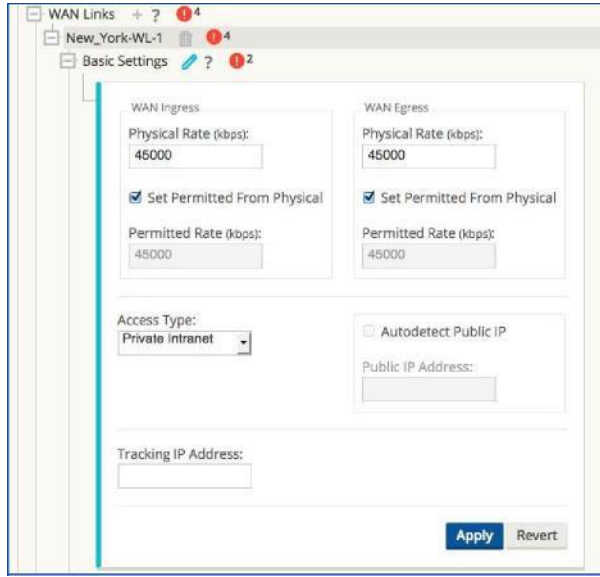
We can use one of our VIPs that we assigned to the site, in this case 10.1.1.11/24. Note we only need to assign one per VI. The other address for the Internet WAN Link will be auto-populated when we create the WAN Link Configuration.

Next we add the WAN Links for the New_York site. There are two sections we need to be concerned with at this time, the basic settings and the access interfaces.

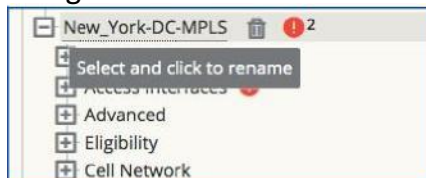
Under basic settings we define the WAN Link bandwidth in each direction.

- WAN Ingress is *To the WAN*
- WAN Egress is *From the WAN*
- The Permitted Rates will be the same as the Physical Rates and are auto-populated
- Since this is an MPLS circuit we set the mode to be private_intranet
- You will notice the WAN Link received an automatic name. We can change this once the basic settings have been applied:

Implementation Guide



Change the name of the WAN Link if desired by clicking on the Name:



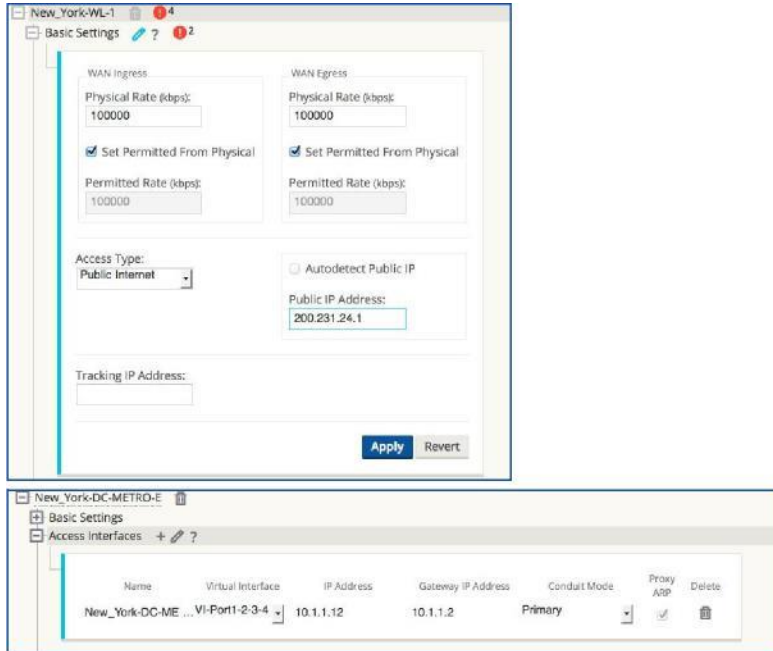
This section defines which Virtual IP we will use for the interface to reach the WAN Link. We will also define the Gateway IP address associated with this interface, WAN Link, and VIP. In the case of a VLAN trunk, create one Access Interface for every VLAN we straddle. Additionally you can select the Proxy ARP mode we would want to use. Proxy ARP allows the Talari to protect against the router failing so that traffic will still flow towards the Talari device and hence into an alternative path if the Conduit is in the good state. The Talari Appliance will respond to ARP requests so the host traffic will be sent off subnet through the Talari Appliance.

Add an Access Interface for the New_York-DC-MPLS WAN Link.

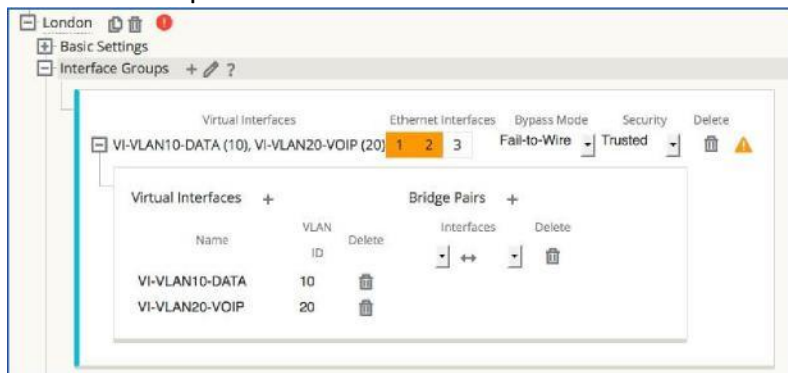


Repeat these steps to add the DC-Metro-E WAN Link. One difference is this WAN Link will be a Public Internet Link and have a public IP address defined. We will use a different VIP 10.1.1.12 under the Access Interface and a different gateway 10.1.1.2.

Implementation Guide



Repeat the above steps for the London Site. Note this will be a client. Additionally the T510 in London straddles a VLAN trunk and hence each VLAN will need to be defined under the Virtual Interface Group as shown below.

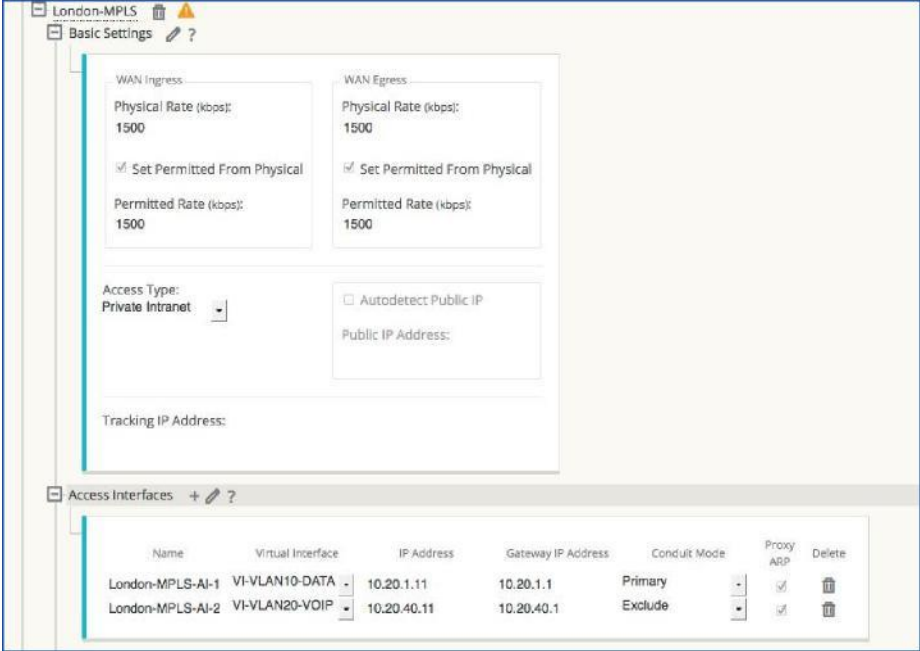


We will also create Virtual IP addresses for each VLAN of interest so we can route traffic correctly to each VLAN subnet.

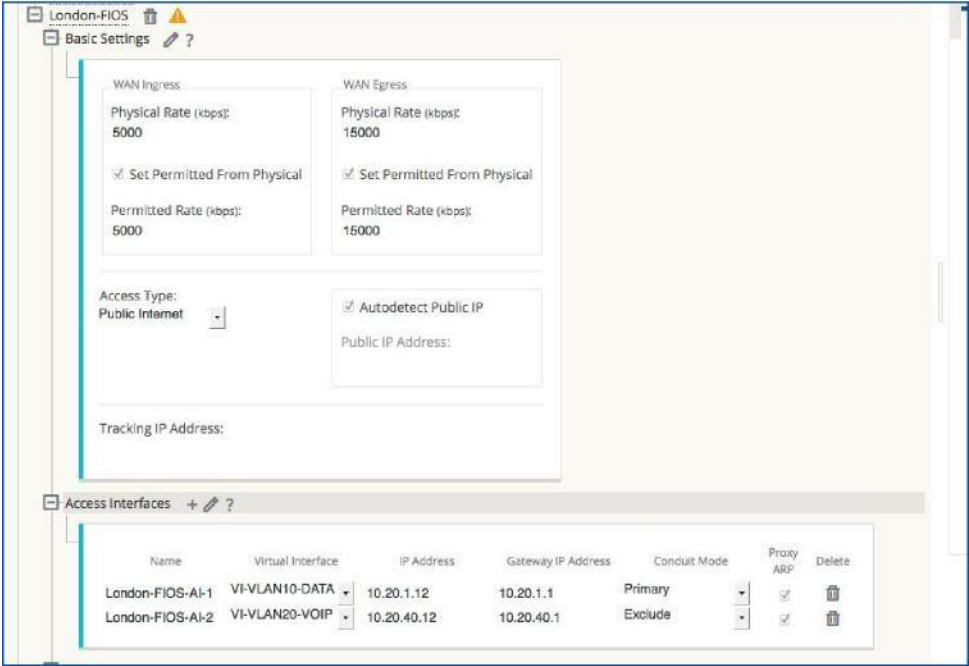


Also we will need Access Interfaces for both VLANs on the WAN Link Definition. Note our 2 WAN Links for London are connected to the same router (more on this later), but they are different WAN Links as one is private Intranet and the other public Internet.

The London MPLS WAN Link:



And the London FIOS WAN Link:



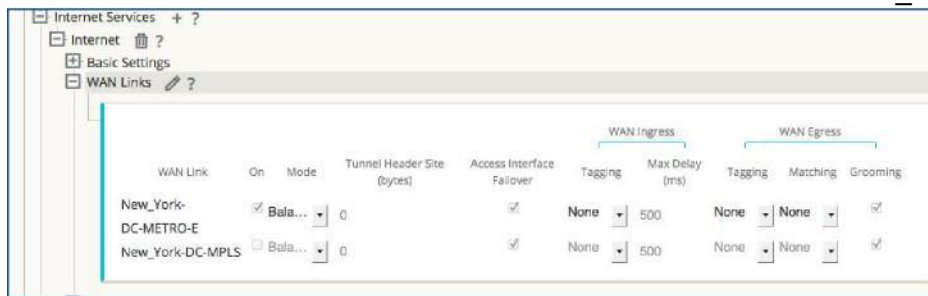
Note: the Conduit mode in most cases is primary. This defines which VLAN we want to establish the Conduit from. We set this to exclude for the other VLANs, so we don't try to establish the

Conduit from that subnet. You will also notice that for London-FIOS we set the public IP address to auto learn. This is useful when the Public IP is dynamically assigned and can change.

Creating the Connections

Our next Step is to create the Conduit connections between our sites, and assign the relevant services to WAN Links. In some cases Conduits are automatically created. For example every site must have a Conduit to the NCN and this is created when the site is built. We can add Conduits to other sites as needed or even turn on Dynamic Conduits. A Conduit is made up of paths between WAN Links at different sites.

In our simple Network our Conduit between New_York and London is already created. We must assign an Intranet Service to the MPLS WAN Links and an Internet Service to the Internet WAN Links. We will start with the Internet Service at New_York.



Note this is only enabled for the New_York-DC-METRO-E WAN Link.

And then we add an Intranet service for New York also, enabling it for the New_York-DC-MPLS WAN Link



Repeat these steps for the London site.

Note: If a site does not deliver traffic to the Internet directly it can be backhauled to another site. For example if Internet access is via a corporate Firewall in the Data center then all traffic is carried across the network via the Conduit. In this case an Internet Service at the remote site is not needed.

Route Configuration

The routes can be defined as Local (LAN) routes, Conduit routes, Intranet routes, Internet routes or Passthrough routes. Each route has a default cost which the user can change if required. Default route

cost is 5. When WAN to WAN forwarding is enabled routes reachable down one Conduit are advertised to the other Conduits in that group with a cost of 10. Talari uses longest prefix matching to determine which route to take. Identical routes are then considered by the route cost, then the service.

A brief description for each mode of route is as follows:

- **Local (LAN) Routes:** Local routes are routes that are local to the site and they reside behind a LAN router. When defining these routes, the user must also define the LAN gateway the appliance will use to get to the route. The appliance needs the next hop gateway IP address to learn what MAC address to forward the frames to. Currently, local routes will be shared between sites that have Conduits (and *only* sites which have Conduits), unless WAN-to-WAN forwarding is enabled.
- **Conduit Routes:** Conduit routes are routes that will traverse the Talari Conduit. When using this route, the user defines the network and subnet, then defines the service mode as Conduit for the route. A cost could then be used versus the default. If a route is desired to traverse a specific Conduit, the user can use this option to provide a better route cost. This, in turn, will force certain traffic down a different Conduit (verses the default Conduit), or provide a backup Conduit if the default Conduit fails.
- **Intranet Routes:** Intranet routes are networks that are not to be used for Conduit services (in other words, sites that are not part of the Talari WAN). These can also be host routes (/32). Note an Intranet route has no Gateway IP address but instead is pointed to the Intranet Service. There can be multiple Intranet Services. The user would configure the network or sub network and mask, then select the service mode to be Intranet. Once complete the user would then select the correct Intranet service defined for the specific route. The Intranet Service must be defined and assigned to a WAN Link for this route to operate correctly. When defining the Intranet Service, be aware of the permitted rate defined on the WAN Link this service is applied to. In certain cases, if an incorrect permitted rate is applied, non-Talari traffic can be adversely impacted. An example would be the Intranet users that are not part of the Talari WAN are seeing slower than normal response times because they do not have enough bandwidth. Be sure to take time and apply the correct permitted rate for the Intranet Service.
- **Internet Routes:** Internet routes are networks that are not to be used for Conduit services. These can also be (/32) routes or host routes. The user would configure the network and mask, select the service mode to be Internet, and define the Gateway and cost. The system adds a default Internet route when the service is enabled for a site. The Internet Service must also be assigned to a WAN Link. Once the Internet Service is defined, a default Internet route is added to the Talari route table.

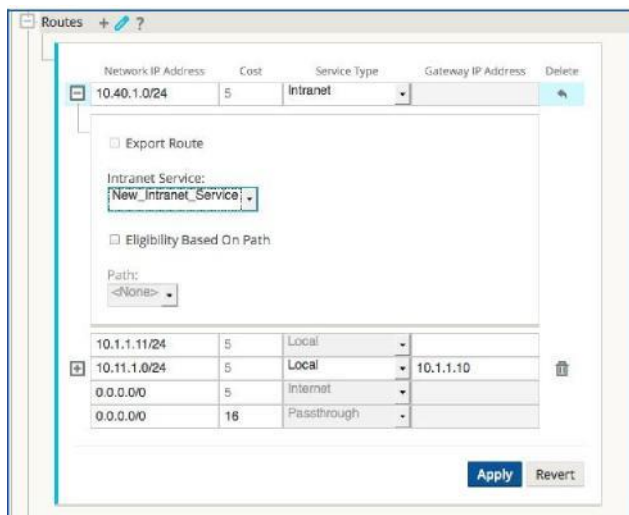
- **Passthrough Routes:** Passthrough routes are routes that do not match Conduit, Intranet, or Internet routes. These routes will not be groomed and will just pass through the appliance. During the initial deployment, the Passthrough Service can be used for traffic to bypass the Conduit.

Once our services have been defined, we can define the additional routes we need for New_York and for London. By default when we create an Internet Service a 0.0.0.0/0 route is created and points toward the WAN Link that the Internet Service is assigned to.

In our example network we need to consider the following:

1. Hong Kong is a Non Talari Site. At Hong Kong we have a subnet 10.40.1.0/24. This still needs to be reachable from both New_York and London. Since there is no Talari in Hong Kong we need to create Intranet routes at New_York and London to route properly to this site.
2. The Local Subnet 10.11.1.0/24 at New_York. This subnet is reached via the local router 10.1.1.10. This also needs to be reachable by London, so we will create a Local route at New_York to accomplish this. Local routes at one site get advertised to the other sites with Talari Appliances as Conduit routes.

Let us add the routes for New_York:



You will notice for the Intranet route this can be exported to other sites if desired. This becomes a Conduit route at that point.

The Local route can also be valid or invalid based on the gateway being reachable:



This step should be repeated for the London Site for the 10.40.1.0/24 Intranet route. Note we don't need to add a route for 10.11.1.0/24 as it will get advertised to us via the Conduit.

Note: There is a catch all route that sends traffic to Passthrough, sometimes it's easier to start with Passthrough to get the configuration running as we won't block traffic that doesn't match the more specific routes. The Internet Service default route will override this catch all.

WAN Link Provisioning

Now that we have our basic configuration complete, we can adjust our provisioning rates for the Conduits and Internet/Intranet Services. By default when these are enabled they are assigned a fair share of the WAN Link bandwidth, with each new service being assigned 1000 shares. The bandwidth assigned is automatically calculated by:

Available Bandwidth (Kbps) / total # of shares X shares assigned to the service/Conduit.

(Available Bandwidth = the WAN Link's Permitted Rate minus the sum of all services' minimum reserved bandwidth.)

Previously we had decided to assign the following ratios to our Services at the New York and London Sites:

| WAN Link Name | WAN Ingress Permitted B/W (Kbps) | WAN Ingress Permitted B/W (Kbps) | Conduit Service Shares | Internet Service Shares | Intranet Service Shares |
|---------------|----------------------------------|----------------------------------|------------------------|-------------------------|-------------------------|
| DC-MPLS | 45000 | 45000 | 30% | N/A | 70% |
| DC-Metro-E | 100000 | 100000 | 50% | 50% | N/A |

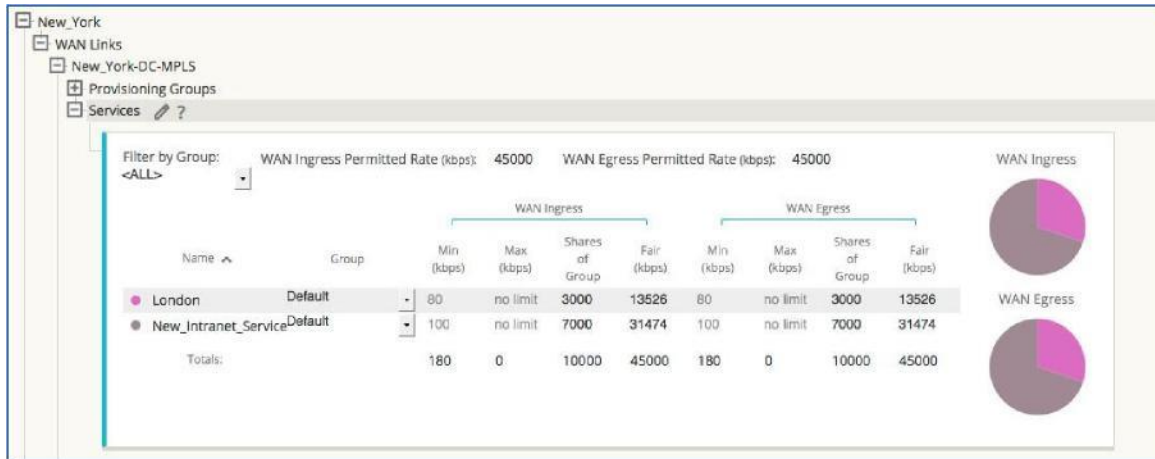
Table 6 WAN Link Configuration for New York (Data Center)

| WAN Link Name | WAN Ingress Permitted B/W (Kbps) | WAN Ingress Permitted B/W (Kbps) | Conduit Service Shares | Internet Service Shares | Intranet Service Shares |
|---------------|----------------------------------|----------------------------------|------------------------|-------------------------|-------------------------|
| LON-MPLS | 1500 | 1500 | 70% | N/A | 30% |
| LON-FIOS | 5000 | 15000 | 50% | 50% | N/A |

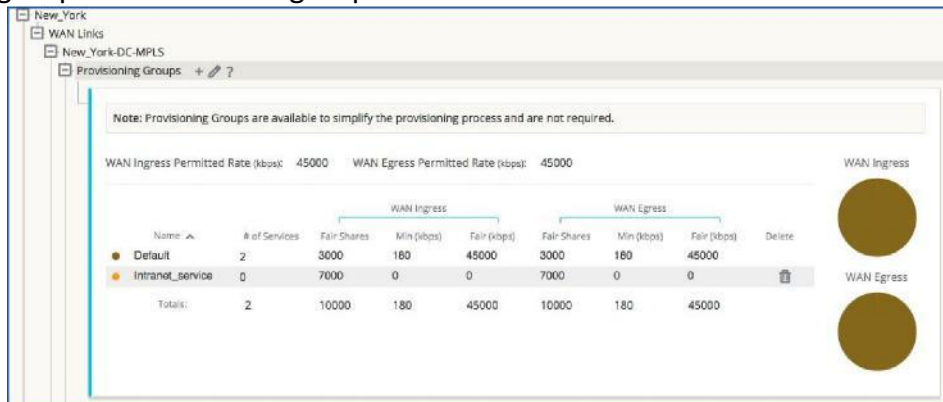
Table 7 WAN Link Configuration for London

Now we need to adjust our provisioning shares to reflect this. Starting with New_York-DCMPLS, under the provisioning tab select services tab and edit the shares of group for both WAN

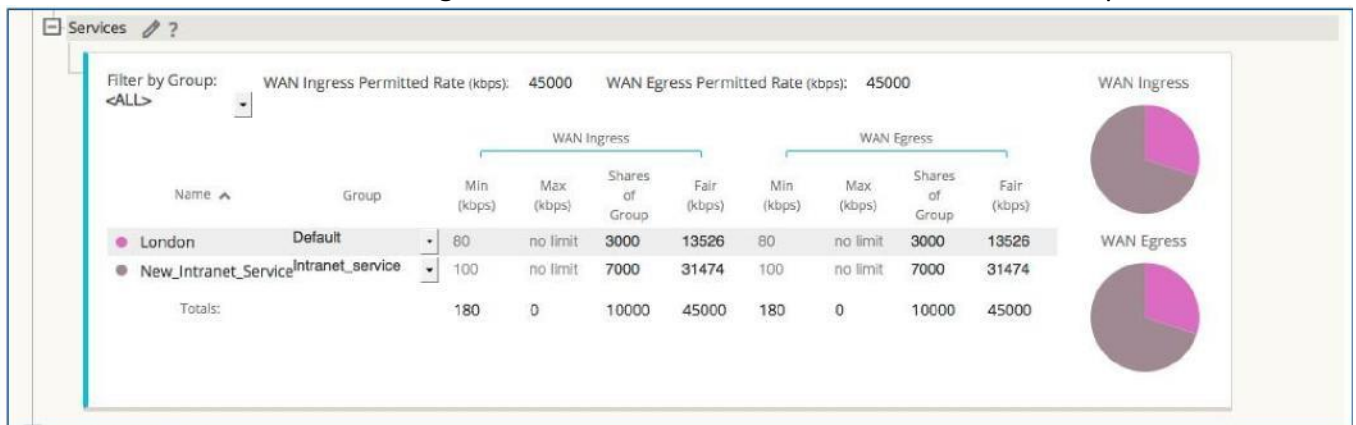
Ingress and WAN Egress to reflect the 30/70 ratio between the Conduit Service and the Intranet Service:



One problem here though, is if we add another site, the ratio will change and no longer be what we want. If we always want the Intranet Service to always have 70% of our bandwidth despite the number of Conduits we must use provisioning groups. Open the provisioning groups tab and add a group for the Intranet Service:



Then under the Services tab – assign the Intranet Service to the Intranet Service Group:



Now no matter how many Conduits get added to this WAN Link the Intranet Service would always have 70% of the total bandwidth.

Note: Most of the time the shares can be left equal as they don't come into effect unless the WAN Link is congested. Additionally the smaller of the two WAN Links determines how much traffic can be sent to a given Site. For example in our network we have 45 Mbps at the Data center and only 1500 Kbps at the client, so even though we allow 13526 Kbps at the Data center for Conduit traffic the most we can send is 1500 Kbps.

We must repeat this for the other WAN Links as necessary to adjust our ratios for the services.

At this point we should have a valid basic configuration. The configuration can be saved and then needs to be exported to change Management to allow the NCN to create the relevant node configuration. Click on the Export button and send the configuration file to the Change Management Inbox. Then go to Manage Network-> Change Management.

Configuration Filenames: Active - DemoConfig_R3_1_broken.cfg Staged - DemoConfig_R3_1_broken.cfg

| Site-Appliance | Model | State | Currently Active | | Currently Staged | | Download Package |
|----------------------|-------|-------|---------------------|-----------------|---------------------|------------------|------------------|
| | | | Software | Config | Software | Config | |
| Raleigh-HA-Prime-App | T750 | | R3_1_QA_D6_02022014 | 16:39 on 2/6/14 | R3_0_GA_P3_01152014 | 20:23 on 1/28/14 | active / staged |
| Raleigh-HA-Sec-App | T750 | | R3_1_QA_D6_02022014 | 16:39 on 2/6/14 | R3_0_GA_P3_01152014 | 20:23 on 1/28/14 | active / staged |
| Sanjose-Sanjose-App | T750 | | R3_1_QA_D6_02022014 | 16:39 on 2/6/14 | R3_0_GA_P3_01152014 | 20:23 on 1/28/14 | active / staged |
| Austin-Austin-App | T730 | | R3_1_QA_D6_02022014 | 16:39 on 2/6/14 | R3_0_GA_P3_01152014 | 20:23 on 1/28/14 | active / staged |
| Chicago-Chicago-App | T510 | | R3_1_QA_D6_02022014 | 16:39 on 2/6/14 | R3_0_GA_P3_01152014 | 20:23 on 1/28/14 | active / staged |

© 2007-2014 Talari Networks. All rights reserved.

Step through the CM process by clicking “Begin”. If this is the first time applying a configuration we will need to load the relevant code images for the Talari Appliances we have, in our case the T5000 and T510. These can be downloaded and can be uploaded individually to the NCN. Simply browse for the images and upload them.

The appliances can then be staged. This part creates the node configuration packages for each appliance. Once the packages are created the remote site package must be downloaded and applied using local change Management on the remote appliance. Once the network is up further changes can be applied automatically.

Policy Based Routing for the Single Router and Multiple WAN Links.

We have finished our configuration for the Talari Appliances but we must now consider infrastructure changes in the network to allow the Talari WAN to function. Let us look at our network diagram again:

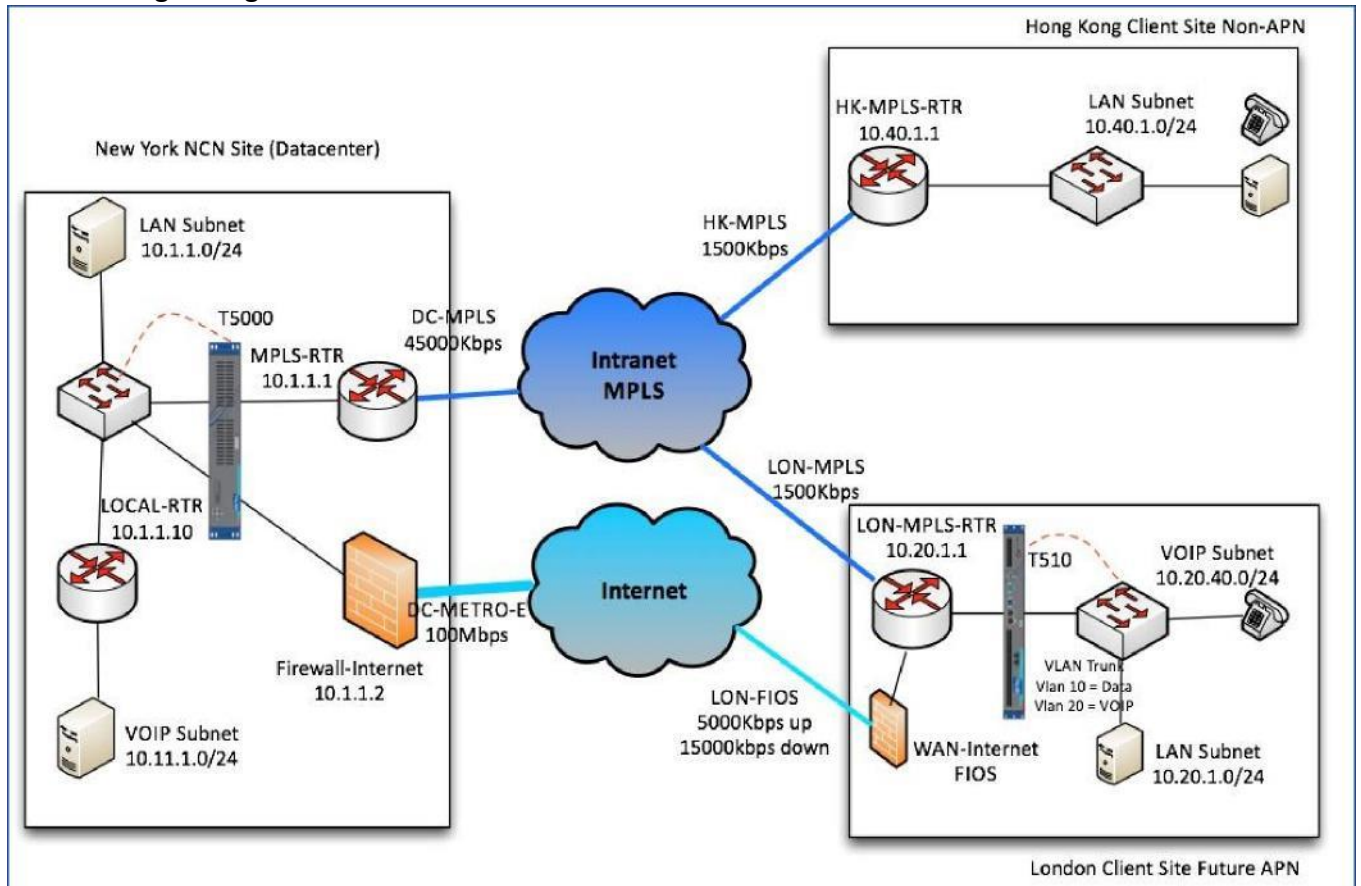


Figure 3 Example Network with Talari Deployed

At the London Site we only have 1 WAN router but two connections. In order for the Talari Paths to function correctly we need to apply a simple Policy Based Route (PBR) map to steer the Conduit packets based on the source address they are coming from. In our example:

- Conduit packets (UDP 2156) from 10.20.1.11 need to always go to the MPLS WAN Link
 - Conduit packets (UDP 2156) from 10.20.1.12 need to always go to the FIOS WAN Link
- If our router is CISCO IOS then we can use a simple PBR route map as shown below to ensure this behavior. In our example the next-hop IP in the cloud for the MPLS router is 100.1.1.2 and the next-hop for the FIOS connection is 203.34.12.276. The route map and access control list would look like this:

```
ip access-list extended CONDUIT-TO-MPLS-acl
permit udp host 10.20.1.11 eq 2156 any ip
access-list extended CONDUIT-TO-FIOS-acl
permit udp host 10.20.1.12 eq 2156 any
```

```
!  
route-map CONDUIT-TO-WAN_LINK permit 10  
match ip address CONDUIT-TO-MPLS-acl  
set interface Null0
```

```
set ip next-hop 100.1.1.2  
!  
route-map CONDUIT-TO-WAN_LINK permit 20  
match ip address CONDUIT-TO-FIOS-acl set  
interface Null0 set ip next-hop 203.34.12.276
```

This would be applied to the VLAN 10 interface of the MPLS router with the command:

```
ip policy route-map CONDUIT-TO-WAN_LINK
```

Note: The command “set interface Null0” is used to eliminate any chance of routing around a failed WAN Link. Since Talari Adaptive Private Networking encapsulation maintains information regarding link latency and jitter, these values would be incorrect or distorted if the network routed around a link failure.

Firewall Rules and NAT

In some cases it may be necessary to create firewall rules and NAT rules to properly map the Talari Traffic back to the Internal VIP addresses. In our example we would need a FW rule at New_York to allow Talari Conduit traffic in from the outside world. By default Talari uses UDP port 2156 as both the source and destination port of every Conduit path. Please refer to *How to Configure Firewalls in a Talari WAN*.

Appendix A - Provisioning

Provisioning allows for the bidirectional (WAN Ingress / WAN Egress) distribution of bandwidth for a WAN Link among the various services associated with that WAN Link. There are two steps to Provisioning that provide for this bandwidth distribution in a simple and effective way:

- **Provisioning Groups** - Create and edit groups of bandwidth. (Optional)
- **Services** - View and edit bandwidth settings for services within a bandwidth group

The Concept of Using Shares

When provisioning bandwidth for networks with a large number of sites, using percentages does not allow for enough granularity as the site count increases. With the Talari provisioning process, we introduce the concept of Fair Shares. Shares are used to distribute the permitted bandwidth over groups, and services within groups.

With shares, the total number of shares is up to the user, allowing any amount of granularity or precision when allocating bandwidth among the different Groups and Services.

Provisioning Groups

A Provisioning Group is a container for an arbitrary collection of Services on any given WAN Link. They allow the user to allocate bandwidth at a high-level before drilling down to the individual Services within the Group for fine-tuning. They also provide a boundary for the automatic redistribution of bandwidth within the child Services of the Provisioning Group.

Note: Provisioning Groups are available to simplify the provisioning process and are not required if they are not needed.

Fair Shares

In the Provisioning Groups table, shares are used to distribute the WAN Ingress/Egress eligible bandwidth, which is the Permitted Rate minus the total Min reserved bandwidth of all Services on the WAN Link. All Services are initially assigned to a **Default Group** that is allocated all of the eligible bandwidth. The user can create additional Groups and allocate bandwidth to its members by giving that Group some number of Fair Shares. The resulting total bandwidth for all Services in the Group is then shown in the Fair (Kbps) column.

Note: All Services receive their Min Reserved Bandwidth before Fair distribution, which could result in Groups with equal Fair Shares having disparate Fair Rates. Fair Rates can also be affected by Service Maximums, if defined.

Services

The **Services** section allows the user to further fine-tune bandwidth allocation. Services that are assigned to the same group contend for the bandwidth allocated by that group. The services shown in the **Services** section of the selected WAN Link have been enabled on that WAN Link by the current Configuration.

By default, all services are assigned to the **Default** group with a default number of fair shares divided evenly among them. The default number of shares serves as a starting point and is not restricted by (nor related to) the number of shares set in the **Provisioning Groups** section.

Default minimum rates by service type:

- **Conduit:** 80 Kbps (including Dynamic Conduit type)
- **Internet/Intranet:** 100 Kbps

Note: To set an unlimited **Max (Kbps)** rate, enter '0' (zero) into the cell.

For the **Dynamic Conduits** service entry (if configured on the selected WAN Link), the **Min (Kbps)** and **Max (Kbps)** fields are variable. Therefore, the range of values that can be expected is shown.

Shares of Group

In the **Services** section, shares are again used to distribute the eligible WAN Ingress/Egress bandwidth. The Group that a service is assigned to determines the eligible bandwidth (listed in

the Fair (Kbps) column in the **Provisioning Groups** section) for all services assigned to the same Group. The Shares of Group are used to divide up the eligible bandwidth among the members of a group based on the ratio of the current service divided by the total number of shares for the group in which it is a member.

The Minimum rate acts as a base bandwidth allocation for each service, and the amount of bandwidth available for fair allocation is based on the total permitted for the group minus the sum of the minimums for each service in the group.

In the case of the **Dynamic Conduits** service, the **Shares of Group** is divided among all Dynamic Conduits. Please refer to the context help for **Dynamic Conduit Provisioning** for more information.

New services enabled on a WAN Link will be placed in the **Default** Group with a **Shares of Group** value of 0 (zero). The **Shares of Group** must be configured to a non-zero value in order to be valid.

When moving a service between Groups, the Service will keep its configured amount of shares. The shares will be removed from the old group and taken to the new Group.

When deleting or disabling a service on a WAN Link, that service's shares will be removed as well. The shares will not be distributed over the remaining services.

Dynamic Conduit Provisioning

The **Dynamic Conduit Provisioning** worksheet is for configuring the parameters of an individual Dynamic Conduit. If a **Dynamic Conduit** service is not enabled on the selected WAN Link, the worksheet will be hidden.

The settings in this worksheet should be treated in the same way as a static Conduit service. Set the **Min (Kbps)** and **Max (Kbps)** for an individual Dynamic Conduit here. Each Dynamic Conduit will use the settings provisioned here. Once the **Min (Kbps)** and **Max (Kbps)** rates have been configured, the **Fair (Kbps)** per Dynamic Conduit will be recalculated to reflect the new settings. Using the Possible Dynamic Conduits and the individual Dynamic Conduit settings in this worksheet, worst-case usages of Min, Max and Fair bandwidth will be calculated. The worstcase Min and Max bandwidth will be shown in the **Min Total (Kbps)** and **Max Total (Kbps)** columns (respectively) in the **Dynamic Conduit Provisioning** worksheet. The worst-case fair bandwidth will be shown in the **Fair (Kbps)** column of the main **Services** table for the **Dynamic Conduits** service.

Note: To set an unlimited **Max (Kbps)** rate, enter '0' (zero) into the cell.

About the Possible Dynamic Conduits Column

The **Possible Dynamic Conduits** value represents the total number of Dynamic Conduits that could exist simultaneously (based on the current Configuration described momentarily). It is either the total number of sites reachable via Dynamic Conduit OR the maximum number of Dynamic Conduits supported by the platform being configured, whichever is fewer. Several

Configuration parameters cooperate to determine if Dynamic Conduits can be created between sites. Sites that have: Dynamic Conduits enabled AND share a common intermediate site with W-T-W Forwarding enabled AND are in the same W-T-W Forwarding group; can establish Dynamic Conduits between each other and are factored into the **Possible Dynamic Conduits** value.

Fair (Kbps)

The fair bandwidth is based on a worst-case scenario in which all accounted Dynamic Conduits are up simultaneously. The number of shares for an individual Dynamic Conduit are used in the calculation. The number of shares for an individual Dynamic Conduit receives in the worst-case is equal to the number of **Shares of Group** defined for the **Dynamic Conduits** service divided by the **Possible Dynamic Conduits**:

For example, if the **Dynamic Conduits** service has 100,000 shares defined for it in the **Shares of Group** column in the Services table, and if the current Configuration accounted for a **Possible Dynamic Conduits** of 4, then 25,000 shares ($100,000 / 4$) will be used as the number of fair shares for an individual Dynamic Conduit.

Once the worst-case number of shares has been calculated, the Fair (Kbps) rate is calculated in the same manner as the other service types.