Chapter 6

Managing Tunnel-Service and IPSec-Service Interfaces

This chapter describes how to configure tunnel-server ports, tunnel-service interfaces, and IPSec-service interfaces on E-series routers.

This chapter contains the following sections:

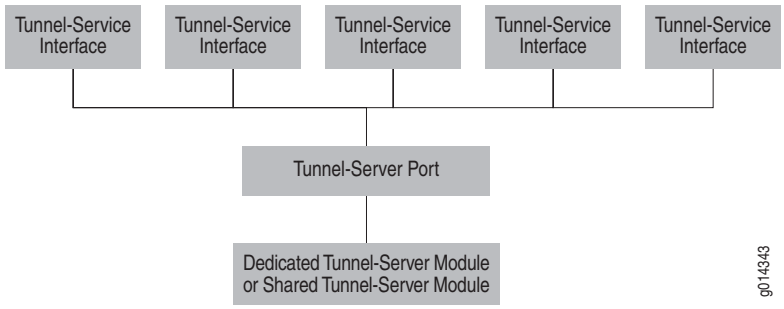
Tunnel-Service and IPSec-Service Overview

Tunnels provide a way of transporting datagrams between routers that do not support the same protocols. Often, these routers are separated by networks.

To configure tunneling, you must identify the tunnel-server ports that reside on modules that support tunnel services. You can then assign the tunnel-service interfaces that encapsulate protocols and enable them to be tunneled across the network.

Figure 35 displays the interface stacking for tunnel-service interfaces on a tunnel-server module.

Figure 35: Interface Stacking for Tunnel-Service Interfaces



This section describes the types of tunnel-server ports that you can configure on tunnel-server modules and the types of tunnel-service interfaces that you can run on these ports.

Types of Tunnel-Server Ports

E-series routers support two types of tunnel-server ports: *dedicated* tunnel-server ports and *shared* tunnel-server ports.

Dedicated Tunnel-Server Ports

Dedicated tunnel-server ports are virtual ports that are always present on dedicated tunnel-server modules. These modules offer only tunnel services; they do not offer access services.

Shared Tunnel-Server Ports

Shared tunnel-server ports are virtual ports that are always present on certain E-series line modules that provide tunnel services in addition to regular access services. You can configure the shared tunnel-server port to use a portion of the module's bandwidth to provide tunnel services.

Shared tunnel-server ports offer the following benefits:

- Greater flexibility in deploying tunnel servers

  You can use a shared tunnel-server module to provide tunnel services as an alternative to using a dedicated tunnel-server module.

- Cost savings

  If you have limited tunnel-server processing needs, you can provide tunnel services on a single available port of a shared tunnel-server module instead of having to allocate the entire bandwidth of a dedicated tunnel-server module for this purpose.

Types of Tunnel-Service Interfaces

You can configure the following types of tunnel-service interfaces using dedicated tunnel-server ports and shared tunnel-server ports:

- Static IP interfaces that you configure and delete

  Static IP interfaces include DVMRP and GRE tunnels. You must assign interfaces on other line modules to act as source endpoints for these tunnels. For information about configuring these tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 10, Configuring IP Tunnels*.

- Dynamic interfaces associated with an L2TP LNS session

  The router establishes dynamic interfaces when required and removes the interfaces when they are not required. For information about applications that use these dynamic interfaces, see *JUNOSe Broadband Access Configuration Guide, Chapter 10, L2TP Overview*.

- Secure IP tunnels

  IPSec-service modules are associated with secure IP tunnels. You must configure and delete these interfaces statically; however, the router assigns tunnels to the interfaces dynamically. This mechanism means that you must manage the interfaces for tunnels manually: however, the router adds and removes tunnels when required. For information about configuring secure IP tunnels, see *JUNOSe IP Services Configuration Guide, Chapter 6, Configuring IPSec*.

Tunnel-Service Interface Platform Considerations

You can configure tunnel-service interfaces on the following E-series routers:

- E120 router
- E320 router
- ERX-1440 router
- ERX-1410 router
- ERX-710 router
- ERX-705 router
- ERX-310 router

This section describes the line modules, I/O modules, and I/O adapters (IOAs) that support tunnel-service interfaces.

For detailed information about the modules that support tunnel-service interfaces on the ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed specifications of these modules.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the protocols and applications that tunnel-service modules support.

For detailed information about the modules that support tunnel-service interfaces on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed specifications of these modules.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the protocols and applications that tunnel-service modules support.

Supported Modules for Dedicated Tunnel-Server Ports

All E-series routers support dedicated tunnel-server ports; however, the supported modules depend on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

ERX-7xx models, ERX-14xx models, and the ERX-310 router all support Service Modules (SMs) and IPSec Service Modules (ISMs).

Unlike other line modules, SMs and ISMs do not pair with corresponding I/O modules that provide ingress and egress ports. Instead, they receive data from and transmit data to other line modules with ingress and egress ports.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that each module supports.

E120 Router and E320 Router

The E120 router and the E320 router support the ES2-S1 Service IOA and ES2 4G line module (LM) combination.

Unlike SMs and ISMs, you must install the ES2-S1 Service IOA with the ES2 4G LM to use dedicated tunnel-server ports. The ES2-S1 Service IOA does not have ingress and egress ports, but it conditions the ES2 4G LM to receive and transmit data to other line modules.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that the ES2-S1 Service IOA supports.

Supported Modules for Shared Tunnel-Server Ports

Most E-series routers support shared tunnel-server ports; however, the supported modules depend on the type of E-series router that you have.

See *JUNOSe Release Notes*, *Appendix A*, *System Maximums* for information about the number of tunnels and sessions that each module supports.

ERX-14xx Models and the ERX-310 Router

The ERX-1440 router and the ERX-310 router support line modules on which you can use shared tunnel-server ports. The following module combinations offer tunnel services in addition to regular access services:

- GE-2 line module with the GE-2 APS I/O module installed
- GE-HDE line module with the GE-2 SFP I/O module installed
- GE-HDE line module with the GE-8 I/O module installed

E120 Router and E320 Router

The E120 router and the E320 router support shared tunnel-server ports on the following line module and IOA combinations:

- ES2 4G LM with the ES2-S1 GE-4 IOA
- ES2 4G LM with the ES2-S1 GE-8 IOA
- ES2 4G LM with the ES2-S1 10GE IOA
- ES2 4G LM with OCx/STMx ATM IOAs
- ES2 4G LM with OCx/STMx POS IOAs

Numbering Scheme

When configuring or managing tunnel-server ports, you must know the numbering scheme for identifying the physical location of the port in the E-series router. The numbering scheme depends on the type of E-series router that you have.

ERX-7xx Models, ERX-14xx Models, and the ERX-310 Router

Use the *slot/port* format to identify dedicated and shared tunnel-server ports.

- *slot*—Number of the slot in which the tunnel-server module resides in the chassis

  In ERX-7xx models, line module slots are numbered 2-6; slots 0 and 1 are reserved for SRP modules. In ERX-14xx models, line module slots are numbered 0–5 and 8–13; slots 6 and 7 are reserved for SRP modules. In an ERX-310 router, line module slots are numbered 1–2; slot 0 is reserved for the SRP module.

- *port*—Number of the port on the tunnel-server module

  For more information about identifying the port number on a tunnel-server port, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

For information about installing tunnel-server modules in ERX routers, see *ERX Hardware Guide, Chapter 4, Installing Modules*.

E120 Router and E320 Router

Use the *slot/adapter/port* format to identify dedicated and shared tunnel-server ports.

- *slot*—Number of the slot in which the line module resides in the chassis

  In the E120 router, line module slots are numbered 0–5. In the E320 router, line module slots are numbered 0–5 and 11–16. For both routers, slots 6 and 7 are reserved for SRP modules; slots 8–10 are reserved for switch fabric modules (SFMs).

- *adapter*—Number of the bay in which the I/O adapter (IOA) resides

  This identifier applies to the E120 and E320 routers only. Dedicated tunnel-server ports are supported on the ES2-S1 Service IOA, which is a full-height IOA and is identified in the software as adapter 0. Shared tunnel-server ports reside on a virtual adapter that is identified in the software as adapter 2.

- *port*—Number of the port on the IOA

  For more information about identifying the port number on a tunnel-server port, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

For information about installing tunnel-server modules in the E120 and E320 routers, see *E120 and E320 Hardware Guide, Chapter 4, Installing Modules*.

Interface Specifier

The configuration task examples in this chapter use the format for ERX-7xx models, ERX-14xx models, and the ERX-310 router to specify a tunnel-server port. (The format is described in *Numbering Scheme* on page 255.)

For example, the following command specifies a dedicated tunnel-server port on port 0 of a tunnel-server module in slot 4.

```
host1(config)#tunnel-server 4/0
```

When you configure a tunnel-server port on an E120 router or an E320 router, you must include the adapter identifier as part of the interface specifier. For example, the following command specifies a dedicated tunnel-server port on port 0 of an ES2-S1 Service IOA installed in both the upper and lower bays of slot 3. (When a full-height IOA is installed in the E120 router or the E320 router, it is identified in the software by the upper adapter bay 0.)

```
host1(config)#tunnel-server 3/0/0
```

For more information about interface types and specifiers on E-series models, see *Interface Types and Specifiers* in *JUNOSe Command Reference Guide, About This Guide*.

Supported Applications for Dedicated and Shared Tunnel-Server Ports

Dedicated and shared tunnel-server ports provide support for some or all of the following applications and services, depending on the capabilities of the tunnel-server module on which the port resides:

- Distance Vector Multicast Routing Protocol (DVMRP) tunnels, also known as IP-in-IP tunnels
- Generic routing encapsulation (GRE) tunnels
- IPSec (on ISMs only)
- Layer 2 Tunneling Protocol (L2TP) network server (LNS) support
- IP packet reassembly for tunnels
- Network Address Translation (NAT)

NOTE: Support for IP reassembly and NAT services on shared tunnel-server ports depends on the capabilities of the module on which the shared tunnel-server port resides.

For a list of applications and services that dedicated and shared tunnel-server modules support on ERX-7xx models, ERX-14xx models, and the ERX-310 router, see *ERX Module Guide, Appendix A, Module Protocol Support*.

For a list of applications and services that dedicated tunnel-server modules support on the E120 and E320 routers, see *E120 and E320 Module Guide, Appendix A, IOA Protocol Support*.

Redundancy and Interface Distribution of Tunnel-Service Interfaces

The redundancy and distribution mechanisms supported for tunnel-service ports configured on ISMs differ from those supported for SMs, the ES2-S1 Service IOA, and shared tunnel-server ports.

This section describes the redundancy and interface distribution mechanisms for all tunnel-server ports.

SMs, ES2-S1 Service IOA, and Shared Tunnel-Server Modules

You can install multiple modules to provide redundancy. If you install multiple modules at the same time, the router automatically distributes the tunnel-service interfaces over the modules in proportion to the available tunnel-service interfaces.

Even distribution of tunnel-service interfaces is not critical to router performance. However, the number of modules that you install must be able to support the extra tunnel if one of the modules becomes unavailable.

NOTE: When both dedicated tunnel-server ports (on SMs) and shared tunnel-server ports (on shared tunnel-server modules) are configured on ERX-7xx models, ERX-14xx models, and the ERX-310 router, the router performs load balancing across all available server ports of the same type. For this purpose, dedicated tunnel-server ports (on SMs) and shared tunnel-server ports (on shared tunnel-server modules) are considered one type of server port, whereas server ports on ISMs are considered a different type.

Interface allocation depends on the types of tunnel-service interface created on the router. For more information about the types of tunnel-service interfaces, see *Types of Tunnel-Service Interfaces* on page 253.

Static IP Tunnel-Service Interfaces

You can configure and delete static IP tunnel-service interfaces.

When you configure a static tunnel-service interface, the router automatically assigns that interface to a particular module. If that module becomes unavailable, the router attempts to reassign the interface to an available module. If no module is currently available, the router keeps track of the interface and assigns it to a module when one become available.

Consequently, if you reinstall a module that was formerly unavailable or removed, the distribution of static tunnel-service interfaces over the modules might be uneven. Because users create and remove static tunnels, the distribution might remain uneven indefinitely.

Dynamic Tunnel-Service Interfaces

The router dynamically creates and deletes dynamic tunnel-service interfaces as dictated by the operation of the relevant protocols. Currently, L2TP sessions are the only dynamic tunnel-service interfaces available.

When the router creates a dynamic tunnel-service interface, it assigns that interface to a particular module. If that module becomes unavailable, the router removes the interface. If the initiator of the dynamic interface requests its reestablishment, the router recreates the dynamic tunnel service interface and assigns it to an available module.

Going forward, if you reinstall a module that was formerly unavailable or removed, the router deletes unwanted dynamic tunnel-service interfaces and creates new ones for applications on other modules. Gradually, the distribution of dynamic tunnel-service interfaces on the modules becomes even.

Interface Allocation for Shared Tunnel-Server Modules

When determining how to distribute interfaces across tunnel-server ports, the E-series router does not perform interface policing to prevent the access services of a shared tunnel-server module from depriving the tunnel services of the requisite interface resources (and vice-versa). We recommend that when provisioning shared tunnel-server ports, you restrict the number of interfaces configured for both access and tunnel services to prevent competition between them.

For example, when paired with the ES2-S1 OC3-8/STM1 IOA or the ES2-S1 GE-4 IOA, the ES2 4G LM on the E320 router can support a maximum of 16,000 access interfaces and 8,000 shared tunnel-server interfaces, both of which must compete for the overall supported maximum of 16,000 interface columns.

For tunneling, PPP, and IP maximums, see *JUNOSe Release Notes, Appendix A, System Maximums*.

ISMs

You can install multiple ISMs to provide redundancy. If you install multiple ISMs at the same time, the router automatically distributes ISM interfaces over the modules in proportion to the available ISM interfaces.

Even distribution of ISM interfaces is not critical to router performance. However, the number of ISMs that you install must be able to support the extra tunnels if one of the modules becomes unavailable.

When you configure a static IPSec interface, the router automatically assigns that interface to a particular ISM. If that ISM becomes unavailable, the interface becomes not present (operational state down).

The router then manages the interface as follows:

- If the interface's local IP address (tunnel source) is less than the remote IP address (tunnel destination), the router attempts to reassign the interface to an available ISM. If the reassignment is successful, the router immediately initiates an IPSec negotiation, also known as *rekeying* the interface.

- If the interface's local IP address is greater than the remote IP address, the router attempts to reassign the interface to an available ISM. If the reassignment is successful, the router waits 3 minutes before initiating an IPSec negotiation.

In either case, the interface becomes available (operational state up) when the rekeying operation is completed successfully. If the rekeying operation fails for reasons such as an unreachable remote end or a policy mismatch, the router waits a certain number of minutes and then tries again.

The wait time increases after each unsuccessful rekeying attempt, and follows a progressive pattern. This pattern gradually increases in intervals, starting at 1 minute and reaching a maximum interval of 60 minutes. The 60-minute interval repeats indefinitely. When the rekeying operation is completed successfully, the pattern starts again.

If no ISM is available to which the router can reassign the interface, the interface remains in the not present state until an ISM becomes available. As a result, the distribution of dedicated ISM interfaces over the modules might become uneven.

Tunnel-Service Interface Considerations

To configure a tunnel-server port, you assign the maximum number of tunnel-service interfaces to run on the specified tunnel-server port. This process is referred to as *provisioning*. Conversely, the process of reducing the maximum number of tunnel-service interfaces on a tunnel-server port to zero is referred to as *unprovisioning* the port.

This section describes the considerations for provisioning and unprovisioning tunnel-service interfaces on dedicated and shared tunnel-server ports.

For instructions on how to provision and unprovision tunnel-service interfaces, see *Configuring Tunnel-Server Ports and Tunnel-Service Interfaces* on page 262.

Provisioning Tunnel-Service Interfaces

By default, dedicated tunnel-server ports are configured to have the maximum number of tunnel-service interfaces that the dedicated tunnel-server module supports. You can reduce the maximum number of interfaces or completely unprovision the port by issuing the **max-interfaces** command.

By default, shared tunnel-server ports are configured to have no tunnel-service interfaces. To provision tunnel-service interfaces on shared tunnel-server ports, you must provision the port by assigning a nonzero maximum number of tunnel-service interfaces to run on the port by issuing the **max-interfaces** command.

Bandwidth Limitations of Shared Tunnel-Server Ports

Bandwidth limitations for shared tunnel-server ports and tunnel-service interfaces depend on bandwidth restrictions, if any, that are in effect for the module on which the shared tunnel-server port resides.

Exchanging Tunnel-Server Modules

Tunnel-server modules are available in different hardware revisions that support varying numbers of tunnel-service interfaces. For more information about determining the hardware revision on a module, see *ERX Module Guide, Table 1, Module Combinations*, or *E120 and E320 Module Guide, Table 1, Modules and IOAs*.

When you exchange a tunnel-server module with a lower capacity for tunnel-service interfaces with a module that supports a higher capacity, the tunnel-server port maintains the original number of provisioned tunnel-service interfaces. By using the **all-available** keyword with the **max-interfaces** command, you can configure the tunnel-server port to automatically adjust the number of provisioned tunnel-service interfaces to the maximum value supported by the new module.

When you exchange a tunnel-server module that has a higher number of provisioned interfaces than the new module's capacity, the module adjusts the provisioned number of interfaces to the maximum value that the module supports.

Table 24 displays sample capacity, configuration, and utilization values for exchanging tunnel-server modules with different capacities.

Table 24: Sample Capacity, Configuration, and Utilization Values for Tunnel-Service Interfaces

Old Capacity	Old Provisioned Interfaces (max-interfaces command)	Old Utilization	New Capacity	New Provisioned Interfaces (max-interfaces command)	New Utilization
8000	5000	5000	16,000	5000	5000
8000	8000	8000	16,000	8000	8000
8000	all-available	8000	16,000	all-available	16,000
16,000	5000	5000	8000	5000	5000
16,000	16,000	16,000	8000	8000	8000
16,000	all-available	16,000	8000	all-available	8000

Unprovisioned Tunnel-Service Interfaces

Tunnel-server ports exist whether or not they have been configured. This means that you cannot delete a tunnel-server port from a module. However, you can unprovision all of the tunnel-service interfaces on a tunnel-server port by issuing the **no max-interfaces** command or the **no tunnel-server** command.

You can also restore the default configuration by issuing the **default max-interfaces** command. On dedicated tunnel-server ports, the default configuration is the maximum number of interfaces that the port supports. On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces.

NOTE: If the module on which the tunnel-server port resides supports IP reassembly or NAT services, these services become enabled when you provision tunnel-service interfaces on the port. However, when you unprovision tunnel-service interfaces to zero, only IP reassembly is disabled and NAT remains configured in the current release.

Configuring Tunnel-Server Ports and Tunnel-Service Interfaces

This section describes the tasks associated with configuring a tunnel-server port and tunnel-service interface.

Identifying the Physical Location of the Tunnel-Server Port

To display the physical location of the dedicated tunnel-server port on your module, issue the **show tunnel-server config** command.

```
host1#show tunnel-server config

                          Server Ports
                          ------------
                                                Provisioned
  Port      Type      MaximumInterfaces         Interfaces     HwPresent
--------   -------   -----------------         -----------    ---------
Port 2/2   shared       8000                      0              yes
Port 8/0   dedicated    16000                     8000           yes
```

Provisioning the Maximum Number of Interfaces on a Tunnel-Server Port

To provision the maximum number of interfaces on a tunnel-server port:

1. From Global Configuration mode, specify the location of the dedicated tunnel-server port that you want to configure.

   On a dedicated tunnel-server port:

   host1(config)#**tunnel-server 8/0**
   host1(config-tunnel-server)#

   On a shared tunnel-server port:

   host1(config)#**tunnel-server 2/2**
   host1(config-tunnel-server)#

   This command accesses Tunnel Server Configuration mode.

2. Provision the maximum number of tunnel-service interfaces to be used on the dedicated tunnel-server port.

   host1(config-tunnel-server)#**max-interfaces all-available**

NOTE: When you issue the **tunnel-server** command, ensure that you specify the same interface specifier that was displayed for this tunnel-server port in the **show tunnel-server config** command in the output described in *Identifying the Physical Location of the Tunnel-Server Port* on page 262. If you specify an incorrect location for the tunnel-server port, the router displays an error message and rejects the command as invalid.

Verifying the Tunnel-Server Interface Configuration

To verify that you properly provisioned the number of tunnel-server interfaces on the tunnel-server port:

1. From Tunnel Server Configuration Mode, return to Privileged Exec mode.

   host1(config-tunnel-server)#**exit**
   host1(config)#**exit**
   host1#

2. Issue the **show tunnel-server config** command.

```
host1#show tunnel-server config

                          Server Ports
                          ------------
                                        Provisioned
  Port      Type     MaximumInterfaces   Interfaces    HwPresent
--------   -------   -----------------   -----------   ---------
Port 2/2   shared       8000               5000          yes
Port 8/0   dedicated    16000              all-available yes
```

   For more information about using the **show tunnel-server** command, see *Monitoring Tunnel-Service Interfaces* on page 264.

Unprovisioning Tunnel-Service Interfaces

To unprovision the tunnel-service interfaces on a tunnel-server port, use any of the following commands, all of which have the same effect:

- Issue the **no max-interfaces** command from Tunnel Server Configuration mode.

  host1(config-tunnel-server)#**no max-interfaces**

- Issue the **max-interfaces 0** command from Tunnel Server Configuration mode.

  host1(config-tunnel-server)#**max-interfaces 0**

- Issue the **no tunnel-server** command from Global Configuration mode. This command unprovisions the tunnel-service interfaces on the specified tunnel-server port but does *not* delete the port itself.

  host1(config)#**no tunnel-server 2/2**

max-interfaces

- Use from Tunnel Server Configuration mode to provision the maximum number of tunnel-service interfaces to be used on a tunnel-server port.
- Specify an integer in the range 0–16000 to provision the maximum number of tunnel-service interfaces.
- Use the **all-available** keyword to provision the maximum number of tunnel-service interfaces to match the maximum value that the tunnel-server module supports.

- Examples

  host1(config-tunnel-server)#**max-interfaces 5000**
  host1(config-tunnel-server)#**max-interfaces all-available**

- Use the **default** version to restore the default configuration. On dedicated tunnel-server ports, the default configuration is the maximum number of tunnel-service interfaces that the tunnel-service module supports (**all-available**). On shared tunnel-server ports, the default configuration is zero tunnel-server interfaces.
- Use the **no** version to reduce the number of provisioned tunnel-service interfaces to zero. Issuing the **no max-interfaces** command has the same effect as issuing the **max-interfaces 0** command.

tunnel-server

- Use from Global Configuration mode to specify the physical location of the tunnel-server port that you want to configure.
- The **tunnel-server** command accesses Tunnel Server Configuration mode, which enables you to provision the maximum number of tunnel-service interfaces to be used on the tunnel-server port.
- For ERX-7xx models, ERX-14xx models, and the ERX-310 router, use the *slot/port* format.
- For the E120 router and the E320 router, use the *slot/adapter/port* format. On dedicated tunnel-server ports, use adapter 0 and port 0. On shared tunnel-server ports, use adapter 2 and port 0.
- Example

  host1(config)#**tunnel-server 12/2**

- Use the **default** version to restore the default configuration. On dedicated tunnel-server ports, the default configuration is the maximum number of tunnel-service interfaces that the tunnel-service module supports. On shared tunnel-server ports, the default configuration is zero tunnel-service interfaces.
- Use the **no** version to reduce the number of provisioned tunnel-service interfaces to zero.

Monitoring Tunnel-Service Interfaces

You can monitor tunnel-service interfaces by using the **show tunnel-server** command.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

show tunnel-server

- Use to display status and configuration information for dedicated and shared tunnel-server ports and tunnel-service interfaces configured on the router. Unconfigured tunnel-server ports are not displayed in the output.
- You can display information for a specific tunnel-server port or for all tunnel-server ports.
- Use the optional **config** keyword to display information about available and provisioned tunnel-service interfaces on each port, and to indicate whether modules that support the use of dedicated or shared tunnel-server ports are currently installed in the router.
- Field descriptions
  - Port:Appl—Identifier in *slot*/*port* or *slot/adapter/port* format for the module or tunneling application
    - slot—Number of the slot in the chassis where the module resides
    - adapter—Number of the bay in which the I/O adapter (IOA) resides.

      This identifier applies only to dedicated and shared tunnel-server ports configured on the E120 and E320 routers. Dedicated tunnel-server ports are always adapter 0; shared tunnel-server ports are always adapter 2.

    - *port*—Number of the tunnel-server port on the module; for dedicated tunnel-server ports, this is a virtual port number that is always 0; for shared tunnel-server ports, this is a virtual port number dynamically assigned by the router
  - Card Type or Active Type—Type of port: dedicated or shared
  - Oper State or Max State—Physical state of the port or application
    - up—Port or application is available
    - down—Port or application is unavailable
    - present—Module associated with this port is installed
    - not present—Module associated with this port has been removed
    - pending—Router has not yet detected all previously configured modules during a reboot or initial installation of the module
  - Active Interfaces or Interfaces—Number of tunnel-service interfaces currently configured on this port
  - Max Interfaces—Total number of tunnel-service interfaces available on this module
  - Fill—Percentage of available interfaces used by a server port, an application on a server port, an application on all server ports, and all server ports
  - Appl Totals—Statistics for each application

- Server Ports—Displays configuration information about dedicated and shared tunnel-server ports on the router; this display format appears only when the **config** keyword is specified
  - Port—Identifier in *slot/port* format (ERX-7xx models, ERX-14xx models, and ERX-310 routers) or s*lot/adapter/port* format (E120 and E320 routers) for the module on which the tunnel-server port resides
  - Type—Type of tunnel-server port: dedicated or shared
  - MaximumInterfaces—Total number of tunnel-service interfaces available on this module
  - Provisioned Interfaces—Total number of tunnel-service interfaces currently provisioned on this port
  - HwPresent—Indicates whether a module that supports the specified tunnel-server port is currently installed in the router: yes or no

- Example 1—Displays information about a dedicated tunnel-server port on an SM

```
host1#show tunnel-server

                  Card      Oper     Active      Max
   Port:Appl      Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ---------- ---------- ----
       Port 8/0 dedicated  present          1       8000 0.0%
   ipsec-tunnel               down          0          0 0.0%
ipsec-transport               down          0          0 0.0%
           l2tp                 up          0       8000 0.0%
      gre/dvmrp                 up          1       4000 0.0%
    Appl Totals
   ipsec-tunnel                             0          0 0.0%
ipsec-transport                             0          0 0.0%
           l2tp                             0       8000 0.0%
      gre/dvmrp                             1       4000 0.0%
          total                             2      12000 0.0%
```

- Example 2—Displays information about a dedicated tunnel-server port on an ISM

```
host1#show tunnel-server

Card      Oper     Active      Max
   Port:Appl       Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ---------- ---------- ----
       Port 2/0 dedicated  present          1       8000 0.0%
   ipsec-tunnel                up          0          0 0.0%
ipsec-transport               down          0          0 0.0%
           l2tp               down          0       8000 0.0%
      gre/dvmrp                 up          1       4000 0.0%
    Appl Totals
   ipsec-tunnel                             0          0 0.0%
ipsec-transport                             0          0 0.0%
           l2tp                             0      16000 0.0%
      gre/dvmrp                             2       8000 0.0%
          total                             2      16000 0.0%
```

- Example 3—Displays information about a specific shared tunnel-server port

```
host1#show tunnel-server 2/2

                 Card      Oper     Active      Max
   Port:Appl     Type      State  Interfaces Interfaces Fill
--------------- ---------  ------- ---------- ---------- ----
       Port 2/2   shared   present          0       4000 0.0%
   ipsec-tunnel               down          0          0 0.0%
ipsec-transport               down          0          0 0.0%
           l2tp                 up          0       4000 0.0%
      gre/dvmrp                 up          0       4000 0.0%
```

- Example 4—Displays configuration information about dedicated and shared tunnel-server ports

```
host1#show tunnel-server config

                        Server Ports
                        ------------
                                          Provisioned
  Port      Type     MaximumInterfaces   Interfaces    HwPresent
--------   -------   -----------------   -----------   ---------
Port 2/2   shared       8000               4000          yes
Port 8/0   dedicated    16000              16000         yes
```