Cisco ASR 901 Router Overview

Cisco ASR 901 Mobile Wireless Router is a cell-site access platform specifically designed to aggregate and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G radio access network (RAN). The Cisco ASR 901 is availabe in the following models:

- Cisco ASR 901-TDM version (A901-12C-FT-D, A901-4C-FT-D, A901-6CZ-FT-D, A901-6CZ-FT-A)
- Cisco ASR 901-Ethernet version (A901-12C-F-D, A901-4C-F-D, A901-6CZ-F-D, A901-6CZ-F-A)

The Cisco ASR 901 router helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using HSPA or LTE, Base Transceiver Stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Code Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment.

The Cisco ASR 901 router transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1/E1 circuits, including leased line, microwave, and satellite. It also supports alternative backhaul networks, including Carrier Ethernet and Ethernet in the First Mile (EFM).

The Cisco ASR 901 router also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport.

Custom designed for the cell site, the Cisco ASR 901 features a small form factor, extended operating temperature, and cell-site DC input voltages.

The Cisco ASR 901 TDM version provides 12 Gigabit Ethernet ports, 16 T1/E1 ports and one Management port. Whereas, the Cisco ASR 901 Ethernet version does not contain the 16 T1/E1 ports. It has only 12 Gigabit Ethernet ports and one management port.

The Cisco ASR 901 router supports Ethernet Virtual Circuits (EVC) only. Metro-Ethernet Forum (MEF) defines an Ethernet Virtual Connection as an association between two or more user network interfaces identifying a point-to-point or multipoint-to-multipoint path within the service provider network. An EVC is a conceptual *service pipe* within the service provider network.

Introduction

A RAN is typically composed of thousands of BTSs or Node Bs, hundreds of base station controllers or radio network controllers (BSCs or RNCs), and several mobile switching centers (MSCs). The BTS or Node Bs

and BSC or RNC are often separated by large geographic distances, with the BTSs or Node Bs located in cell sites uniformly distributed throughout a region, and the BSCs, RNCs, and MSCs located at suitably chosen Central Offices (CO) or mobile telephone switching offices (MTSO).

The traffic generated by a BTS or Node B is transported to the corresponding BSC or RNC across a network, referred to as the backhaul network, which is often a hub-and-spoke topology with hundreds of BTS or Node Bs connected to a BSC or RNC by point-to-point time division multiplexing (TDM) trunks. These TDM trunks may be leased-line T1/E1s or their logical equivalents, such as microwave links or satellite channels.

The Cisco ASR 901 has two different types of interfaces by default: network node interfaces (NNIs) to connect to the service provider network and user network interfaces (UNIs) to connect to customer networks. Some features are supported only on one of these port types. You can also configure enhanced network interfaces (ENIs). An ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), EtherChannel Link Aggregation Control Protocol (LACP).

Features

This section contains the following topics:

Performance Features

- Autosensing of port speed and autonegotiation of duplex mode on all ports for optimizing bandwidth.
- Automatic-medium-dependent interface crossover (auto-MDIX) capability on 100 and 100/1000 Mbps interfaces and on 100/1000 BASE-T/TX small form-factor pluggable (SFP) module interfaces that enables the interface to automatically detect the required cable connection type (straight-through or crossover) and to configure the connection appropriately.
- EtherChannel for enhanced fault tolerance and for providing up to 8 Gbps (Gigabit EtherChannel) or 800 Mbps (Fast EtherChannel) full duplex of bandwidth between switches, routers, and servers.
- Link Aggregation Control Protocol (LACP) for automatic creation of EtherChannel links (supported only on NNIs or ENIs).
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate.

Management Options

- CLI—You can access the CLI either by connecting your management station directly to the router console port or by using Telnet from a remote management station. For more information about the CLI, see Using the Command-Line Interface
- Cisco Configuration Engine—The Cisco Configuration Engine is a network management device that works with embedded Cisco IOS CNS Agents in the Cisco ASR 901 Series Aggregation Services Router software. You can automate initial configurations and configuration updates by generating router-specific configuration changes, sending them to the router, executing the configuration change, and logging the results.

- SNMP—SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager.

For information about configuring SNMP, see http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf014.html.

For the list of MIBs that Cisco ASR 901 router supports, see the Release Notes for Cisco ASR 901 router.

Manageability Features

- Address Resolution Protocol (ARP) for identifying a router through its IP address and its corresponding MAC address.
- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the router and other Cisco devices on the network (supported on NNIs by default, can be enabled on ENIs, not supported on UNIs).
- Network Time Protocol (NTP) for providing a consistent time stamp to all routers from an external source.
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the router uses.
- In-band management access for up to five simultaneous Telnet connections for multiple CLI-based sessions over the network. Effective with Cisco IOS Release 15.3(2)S1, in-band management access for up to 98 simultaneous Telnet connections for multiple CLI-based sessions over the network.
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network.
- In-band management access through SNMP Versions 1 and 2c get and set requests.
- Out-of-band management access through the router console port to a directly attached terminal or to a remote terminal through a serial connection or a modem.
- User-defined command macros for creating custom router configurations for simplified deployment across multiple routers.
- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge devices, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and IEEE 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback (requires the metro IP access or metro access image).
- Configuration replacement and rollback to replace the running configuration on a router with any saved Cisco IOS configuration file.
- CPU utilization threshold logs.

Security Features

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes.

- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process.
- Multilevel security for a choice of security level, notification, and resulting actions.
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs or ENIs.
- TACACS+, a proprietary feature for managing network security through a TACACS server.
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through authentication, authorization, and accounting (AAA) services.
- Extended IP access control lists for defining security policies in the inbound direction on physical ports.
- Extended IP access control lists for defining security policies in the inbound and outbound direction on SVIs.

Quality of Service and Class of Service Features

- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue.
- Cisco modular quality of service (QoS) command-line (MQC) implementation
- Classification based on IP precedence, Differentiated Services Code Point (DSCP), and IEEE 802.1p class of service (CoS) packet fields, or assigning a QoS label for output classification
- Policing
  - One-rate policing based on average rate and burst rate for a policer
  - Two-color policing that allows different actions for packets that conform to or exceed the rate
  - Aggregate policing for policers shared by multiple traffic classes
- Table maps for mapping CoS, and IP precedence values
- Queuing and Scheduling
  - Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
  - Port shaping to specify the maximum permitted average rate for a port
  - Class-based weighted queuing (CBWFQ) to control bandwidth to a traffic class
  - Low-latency priority queuing to allow preferential treatment to certain traffic
- Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface.

Layer 3 Features

- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - OSPF

  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, and BGP routing protocols
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and router solicitation messages to discover the addresses of routers on directly attached subnets

Layer 3 VPN Services

These features are available only when the router is running the Advance Metro IP services.

- Multiple VPN routing/forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple virtual private networks (VPNs) and overlap IP addresses between VPNs.
- MPLS VPN is supported.

Monitoring Features

- Router LEDs that provide port- and router-level status
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Enhanced object tracking for HSRP clients (requires metro IP access image)
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring (requires metro IP access or metro access image)
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover (requires metro IP access or metro access image)
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down (requires metro IP access or metro access image)
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy (requires metro IP access or metro access image)