CHAPTER 1

Terms and Concepts

This module defines terms and concepts that are necessary for understanding the Login Event Generators (LEGs) and the Subscriber Manager (SM) configuration and operation. More information about all items can be found in the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

General Concepts

Cable/Satellite Modem

A data modem that provides Internet access over cable and satellite networks. The modem usually corresponds to a single subscriber of the Internet Service Provider (ISP).

CPE (Customer Premise Equipment)

Any equipment that an end-user can connect to the network through a modem. The end-user usually owns multiple CPE devices that are used to connect to the Internet through a single modem.

LEG (Login Event Generator)

A software component that performs subscriber login and logout operations on the SM/SCE. The LEG handles dynamic subscriber integration.

Pull-request

A message sent from a service control engine (SCE) platform to the SM or the LEG when it identifies the use of a new subscriber IP address in the network. The SM uses the IP address provided in this message to query the database to retrieve the subscriber data of the subscriber associated with this address and to send its data to the SCE.

RDR (Raw Data Record)

A client/server data protocol that enables the SCE devices to export reports about network transactions to external collectors. This is a Cisco proprietary protocol.

Subscriber Domain

The SM provides the option of partitioning SCE platforms and subscribers into subscriber domains. A subscriber domain is a group of SCE platforms that share a group of subscribers. Subscriber domains can be configured using the SM configuration file and can be viewed using the SM Command-Line Utility (CLU).

It is also possible to configure domain aliases. A domain alias is a synonym for the actual domain name in the SM. Domain aliases are configured in the SM configuration file.

For additional information about domains and domain aliases, see the "Configuration File Options" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Subscriber ID

The Service Control solution requires a unique identifier for each subscriber. A subscriber ID represents a logical subscriber entity from the service provider perspective.

Subscriber Mappings

The SCE platform requires mappings between the network IDs (IP addresses) of the flows it encounters and the subscriber IDs. The SM database contains the network IDs that map to the subscriber IDs. The SCE network-ID-to-subscriber mappings are constantly updated from the SM database.

The main function of the SM LEGs is to provide the SM/SCE with network-ID-to-subscriber mappings in real time.

For information about the SCE platforms, see the *Cisco SCE 1000 2xGBE Installation and Configuration Guide* and the *Cisco SCE 2000 4xGBE Installation and Configuration Guide*.

CNR Concepts

Communication Link Failure Handling

A keep-alive mechanism periodically checks the communication link (socket) between the CNR LEG and the SM. The communication link fails when the socket is closed or a keep-alive timeout occurs. You can configure the keep-alive timeout in the SM configuration file.

In cases where a LEG to SM link fails, you can configure the SM to clear the mappings of all the subscribers that are updated by the failed LEG.

To learn more about communication link failure handling, see the "Configuration File Options" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

DHCP DoS Attack Filter

The connection between the CNR LEG and the SM is a resource that should be protected against DHCP Denial of Service attacks. Such attacks are dispatched by sending a high rate of DHCP requests from a certain subscriber, which can cause the connection to overflow because of too many logon messages in a short period of time. The CNR LEG enables the administrator to use the filter that identifies such events of multiple identical DHCP requests and filters them to reduce the rate of logon messages to a predefined rate. The filter does not protect the CNR against attacks, but rather protects the connection to the SM.

Remote Procedure Call Protocol (PRPC)

The CNR LEG communicates with the SM using a proprietary remote procedure call (PRPC) protocol developed by Cisco. The SM Java, C, and C++ APIs also use PRPC. The CNR LEG uses the C++ API as its communication layer.

SM C++ API

The SM C++ API exposes a set of operations designed to enable subscriber integration with the Cisco system. The CNR LEG uses the SM C++ API as its basic communication layer.

For additional information about the C++ API, see the *Cisco SCMS SM C/C++ API Programmer Guide*.

SM Cable Support Module

The cable support module is an SM component that executes an API friendly to cable environment integrations. The cable support module translates between the cable subscriber terminology (CPE, CM, and CMTS) and the generic subscriber terms used by the Cisco Service Control Management system. The CNR LEG uses PRPC to invoke the **cableLogin** and **cableLogout** operations that are performed by the cable support module API.

The SM cable support module is used only in the CPE as Subscriber mode.

For additional information about the cable support module, see the "CPE as Subscriber in Cable Environment" chapter of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

Subscriber Autologout

The SM supports the configuration of an autologout timer (lease-time) for each subscriber. The timer is set when performing a subscriber **cableLogin** or **login** operation. The CNR LEG extracts and sets an autologout value from the DHCP IP lease expiration time option.

Subscriber Mode

The Subscriber Mode defines which entity is referred to as the subscriber in the LEG and in the SM.

Cable providers usually prefer using the Cable Modem (CM) as the subscriber entity to be assigned multiple IP addresses (one per Customer Premises Equipment (CPE)).

The CNR LEG supports the CPE as Subscriber and CM as Subscriber (the default) modes, as defined by the configuration.

The CNR LEG works with the SM cable support module when operating in the "CPE as Subscriber" mode. For additional information about cable environment subscriber modes, see the the "CPE as Subscriber in Cable Environment" module of the *Cisco Service Control Management Suite Subscriber Manager User Guide*.

DHCP Concepts

DHCP ACK Packet

The final packet that is transmitted from the DHCP server in each DHCP transaction (except the release transaction). After the transmission of the DHCP ACK packet, the results of the transaction are final.

DHCP Lease Extension Transaction (Renewal)

A DHCP transaction for renewal of the entity lease time. When the lease time has been reached, the network entity is removed from the network. The LEG uses this query to logon the subscriber using the new lease time.

DHCP Lease Query Transaction

The DHCP Lease Query transaction is a DHCP transaction with special message types that enable, among other things, clients to query DHCP servers regarding the owner and the lease-expiration-time of an IP address.

An IETF standard defines the DHCP Lease-Query transaction. For more information, see the IETF website.

DHCP Release Transaction

A DHCP transaction for releasing IP addresses. This transaction is used to logout network entities from the network. The DHCP release transaction is rarely used. Logout is usually performed when the lease time expires, and not directly with a release transaction. The LEG uses the release query to logout a subscriber from the SM.

DHCP Sniffer

The software logic inside the SCE device that analyzes DHCP traffic and sends the information to the SCE-Sniffer DHCP LEG using the raw data record (RDR) protocol.

Subscriber Policy

A subscriber policy package usually defines the policy enforced by Cisco SCMS solutions on each subscriber. The DHCP Lease Query LEG and the SCE-Sniffer DHCP LEG can handle the package ID in any of the following ways:

- Set the policy according to configurable options of the DHCP initial login or lease extension transactions
- Set the policy using a constant default value
- Leave the policy unset

For additional information, see the *Cisco Service Control Application for Broadband User Guide*.

RADIUS Concepts

NAS (Network Access System)

A network device that serves as an access point for a remote user. It initiates RADIUS transactions to the RADIUS server to authenticate a remote user.

The RADIUS Listener LEG refers to all of its RADIUS clients as NAS devices, even though they might be RADIUS servers acting as a proxy or forwarding messages.

RADIUS Accounting Transactions

The RADIUS accounting transactions are used to keep track of the services used by the user for administrative purposes. The LEG supports RADIUS accounting based on RFC 2866. The only RADIUS accounting packet the LEG uses is ACCOUNTING-REQUEST.

RADIUS Accounting Start/Interim/Stop

The RADIUS Accounting messages must hold an attribute called Acct-Status-Type. This attribute can receive the value of **start**, **interim-update**, **stop**, or other RADIUS Accounting messages. An Accounting-Start message contains the Acct-Status-Type with the value **start**.

For additional information, see the relevant RADIUS RFC documentation.

RADIUS Authentication Transactions

The RADIUS transactions are used for authenticating a remote user, and authorizing access to the network's resources. The LEG supports RADIUS authentication based on RFC 2865. The authentication RADIUS packets used by the LEG are ACCESS-REQUEST and ACCESS-ACCEPT.

RADIUS Sniffer

The software logic inside the SCE device that analyzes RADIUS traffic and sends the information to the SCE-Sniffer RADIUS LEG using the RDR protocol.

Subscriber Mappings over VPN

Starting from version 3.1.5 the RADIUS Listener LEG supports dynamic integration for subscriber mappings over VPN. The LEG can be configured to extract a VLAN-ID from a RADIUS attribute and use it along with the extracted IP address.

Note Currently the LEG supports subscriber mappings over VPN only for VPNs that are defined by a VLAN-ID (also referred to as "VPNs of type VLAN").

Note The SM is able to learn VLAN VPNs automatically: upon subscriber login with a VLAN-ID that is unknown to the SM, the SM will add the VPN automatically using the VLAN-ID as a VPN name

Subscriber Policy

A subscriber policy package usually defines the policy enforced by Cisco SCMS solutions on each subscriber. The RADIUS Listener LEG and the SCE-Sniffer RADIUS LEG can handle the package ID in any of the following ways:

- Set the policy according to configurable attributes of the RADIUS transactions
- Set the policy using a constant default value
- Leave the policy unset

For additional information, see the *Cisco Service Control Application for Broadband User Guide*.

MPLS/VPN BGP Concepts

BGP (Border Gateway Protocol)

An exterior gateway protocol used on the Internet to provide loop-free routing between different autonomous systems.

In the context of MPLS/VPN, the BGP protocol is used to distribute the MPLS/VPN routes of a PE router to its neighboring PE routers.

CE (Customer Edge)

A router on the service provider site that connects to the PE (Provider Edge) router in the MPLS core. The CE router only passes the message packet with the IP address and is not concerned with the MPLS/VPN label.

MPLS (Multi Protocol Label Switching)

A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on pre-established IP routing information.

PE (Provider Edge)

A router in the service provider MPLS core that provides routing information between the customer router and the MPLS/VPN network. The PE router maintains a VRF (Virtual Routing and Forwarding) table for each customer site to determine how to route the packet.

RD (Route Distinguisher)

An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.

The RD uniquely identifies the VPN VRF within a PE router.

RR (Route Reflector)

A network element in the service provider network that is used to distribute BGP routes to the service provider BGP-enabled routers. Route Reflectors provide a mechanism for both minimizing the number of update messages transmitted within the autonomous system and reducing the amount of data that is propagated in each message.

RT (Route Target)

Used by the routing protocols to control import and export policies and to build arbitrary VPN topologies for customers.

VPN ID

The Service Control solution requires a unique identifier for each VPN. A VPN ID represents a logical VPN entity from the service provider perspective.

VPN (Virtual Private Networking)

A technology for securely connecting a computer or network to a remote network over an intermediate network such as the Internet.

VPNs can use an insecure public network such as the Internet to connect two networks. They can also use an insecure public network to connect a network and a remote computer, or employ technologies such as tunneling, encryption, and authentication to secure the connection.

VRF (Virtual Routing and Forwarding)

In general, a VRF includes the routing information that defines the VPN site that is attached to a PE router. A VRF consists of an IP routing table, a forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

SOAP Concepts

SOAP

SOAP is a lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.

UsernameToken Profile

The <wsse:UsernameToken> is an element introduced in the WSS SOAP Message Security documents as a way of providing a username.

WSDL

WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services).

WSS

WS-Security (Web Services Security) is a communications protocol providing a means for applying security to Web Services. Originally developed by IBM, Microsoft, and VeriSign, the protocol is now officially called WSS and is developed and maintained via committee in Oasis-Open.

The protocol contains specifications on how integrity and confidentiality can be enforced on Web Services messaging. WS-Security incorporates security features in the header of a SOAP message and thus works in the application layer. Thus, it ensures end-to-end security.