Cisco Virtual Office: Secure Wireless

Contents

Scope of Document

This deployment guide provides detailed design and implementation information for deployment of secure wireless access with the Cisco® Virtual Office solution.

Please refer to the Cisco Virtual Office overview (http://www.cisco.com/go/cvo) for more information about the solution, its architecture, and all of its components.

Introduction

Cisco Virtual Office is a VPN solution that is intended to provide an office-like environment for teleworkers in remote locations. The solution has been successfully deployed by many customers as well as internally at Cisco. One aspect of the office environment consists of having secure wireless access to the corporate network resources. Cisco Virtual Office provides an extension to the corporate wireless LAN (WLAN), and thus all corporate-validated wireless devices can connect from a small office or home office (SOHO) location.

Enterprise WLANs need strong security policies that protect the company from rogue access points, intruders, unauthorized users, and unauthorized viewing of transmitted data. Cisco supports IEEE 802.1x authentication and numerous Extensible Authentication Protocol (EAP) methods—providing a centrally managed, standards-based,

open wireless network security scheme and also some of the earlier 802.11 Wired Equivalent Privacy (WEP) implementations and Wi-Fi Protected Access (WPA).

The 802.1x standard provides WLANs with strong, mutual authentication between a client and an authentication server, as well as dynamic per-user, per-session encryption keys that remove the administrative burden and security concerns surrounding static encryption keys.

EAP is one implementation of 802.1x for enterprises. It is a standardized authentication framework that comprises different authentication mechanisms, including: Lightweight EAP (LEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Protected EAP (EAP-PEAP), EAP-Transport Layer Security (EAP-TLS), and EAP-Tunneled Transport Layer Security (EAP-TTLS).

This document describes how to configure a Cisco IOS® Software spoke router for Cisco Virtual Office to enable secure wireless access for teleworkers using EAP methods, WPA Pre-Shared Key (WPA-PSK), and WEP. Wireless access includes: wireless Internet connection for PCs and laptops, voice over IP (VoIP) over wireless, and support for dual-mode phones. This guide is not intended to help you set up your devices for wireless connection at your remote location.

Platforms and Images

The platforms and images used in this document follow:

- Spoke router: Cisco 871W and 881W Integrated Services Routers
- Image: Cisco IOS Software Release 15.0(1)M

For a complete list of supported and recommended platforms and images, please refer to “Cisco Virtual Office Supported Hardware and Software” at http://www.cisco.com/go/cvo.

Optional

- Authentication, authorization, and accounting (AAA) server: Cisco Secure Access Control Server (ACS) 5.2
- Wireless IP phones: Cisco Unified Wireless IP Phone 7921G models
- Dual-mode phones
- Wireless printers
- Cisco Wireless LAN Controller (WLC) Module with Code Version 5.1 or later to support the Cisco 881W
- Cisco Wireless Control System (WCS)

Hub Configuration

No special configuration is required on the hub side to provide wireless access for teleworkers.

Spoke Configuration

In order to enable secure wireless access, you must configure an AAA server (either local or remote) on the spoke router. A local AAA server can support either EAP-LEAP or EAP-FAST, whereas a remote ACS can support all EAP methods. For configuring the remote Cisco Secure ACS, please refer to the “Cisco Virtual Office-AAA Deployment” guide at http://www.cisco.com/go/cvo.

The most common deployment for remote wireless access consists of having the teleworkers authenticate their machines with the corporate AAA server, using the same policies as in the office. This authentication is done over

the secure tunnel established between the spoke in the remote location and the hub at the headend. Thus, using a remote ACS is the recommended, widely used scenario.

The remaining spoke wireless configuration is platform-specific because of the differences between the access-point modules on the Cisco 881W and those on the Cisco 871W: the access-point module on the Cisco 871W chassis is a Wi-Fi module that uses the same image and command-line interface (CLI) as the router, whereas the one on the Cisco 881W chassis has its own Cisco IOS Software image and flash memory, independent from the router. You can operate it in either autonomous (standalone) or lightweight (unified) mode. To access the module on the Cisco 881W, establish a reverse Telnet session using the following command on the router, and then provide the appropriate credentials, if any:

```
service-module wlan-ap 0 session
```

To go back to the router CLI, press the escape sequence: CTRL+SHIFT+6 and then press x. To close the session, type “disconnect” on the router prompt, or use the following command:

```
service-module wlan-ap 0 session clear
```

Cisco 871W Integrated Services Router Configuration

To configure wireless access on the Cisco 871W, use the router Cisco IOS CLI.

Bridge groups are used to associate WLAN Service Set Identifiers (SSIDs) with the corresponding VLANs. You must configure a Bridge-Group Virtual Interface (BVI) for each bridge group. This interface represents the bridge group and is used as its default gateway.

The Dot11Radio0 interface is the radio interface of the router and is used for communicating with the wireless clients. Subinterfaces are used to support different bridge groups.

SSIDs are configured on the router, with each SSID representing one WLAN. A one-to-one mapping exists between SSIDs and VLANs configured on the router. In the SSID configuration mode, open EAP authentication is used in order to allow any client that supports any of the EAP methods configured on the ACS to try to authenticate. Recall that only EAP-LEAP and EAP-FAST are supported by a local AAA server, whereas all EAP methods are possible on an external ACS. If an external ACS is used, EAP-PEAP is the recommended, most popular EAP method used by wireless clients because it provides higher security by using certificates to authenticate the ACS and optionally the client machines (PEAP-EAP-TLS).

Following is the full wireless configuration on the Cisco 871W spoke router.

For a detailed explanation of CLI commands, please refer to the CLI Command Lookup Tool. You must have a valid Cisco.com account to log in to this page.

```
!!AAA server configuration!!
aaa new-model
aaa group server radius <aaa-group-name>
 server-private <aaa-server-address> auth-port 1812 acct-port 1813 key 0
<server-key>
aaa authentication login eap <eap-list-name> group <aaa-group-name>
```

```
aaa authorization exec default local
ip radius source-interface BVI1
```

Note that if you use a local RADIUS server, you must add the following configuration to create that server. Add as many users as needed by using the **username** <user> **password** <password> command:

```
radius-server local
  nas <bvi1-address> key 0 <server-key>
  username <user> password 0 <password>

!!SSID configuration with open EAP authentication and WPA for key-
  management!!
 dot11 ssid corporate
   vlan 10
   authentication open eap <eap-list-name>
   authentication key-management wpa optional
```

If LEAP is a supported authentication method, you must also add the following command to the SSID configuration:

```
authentication network-eap <eap-list-name>

!!DHCP pool that assigns IP addresses to the wireless clients!!
 ip dhcp pool client
   import all
   network <subnet-address> <subnet-mask>
   domain-name cisco.com
   option 150 ip <tftpserver-address-for call manager>
   netbios-name-server <netbios-address>
   dns-server <dnsserver-address>
   default-router <bvi1-address>
   update arp

!!Dot11radio0 interface. Note that a suitable encryption cipher suite
  must be specified since WPA is used for key-management!!
interface Dot11Radio0
 no ip address
 !
 encryption vlan 10 mode ciphers aes-ccm tkip wep128
 !
 broadcast-key vlan 10 change 600
 !
 !
 ssid corporate
 !
 speed basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
```

```
 station-role root

!!Sub-interface in bridge-group 1!!
interface Dot11Radio0.1
 encapsulation dot1Q 10
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding

!!Vlan associated with bridge-group 1!!
interface Vlan10
 no ip address
 no autostate
 bridge-group 1
 bridge-group 1 spanning-disabled

!!BVI1 interface!!
interface BVI1
 description inside interface
 ip address <bvi1-address> <subnet-mask>
```

Note: You can also use WPA-PSK and WEP for authenticating wireless clients. However, this deployment would be less secure than using EAP and is not recommended for corporate access. Please refer to the “Guest Access” section of this document for WPA-PSK and WEP configuration on the spoke router.

Cisco 881W Integrated Services Router Configuration

To provide wireless access to teleworkers, the Cisco 881W Integrated Services Router uses an access-point service module that runs its own image and has its own flash memory, independent from the router. This access-point module supports IEEE 802.11n, thus providing a higher capacity and better security.

On the router side, BVIs are not configured on the Cisco 881W. VLAN interfaces are used instead, as follows:

```
interface Vlan10
 description Data VLAN to used with wireless
 ip address <vlan10-address> <subnet-mask>
```

You must configure a Dynamic Host Configuration Protocol (DHCP) pool on the router to provide IP addresses for clients:

```
ip dhcp pool client
   import all
   network <subnet-address> <subnet-mask>
   domain-name cisco.com
   option 150 ip <tftpserver-address-for call manager>
```

```
    netbios-name-server <netbios-address>
    dns-server <dnsserver-address>
    default-router <vlan10-address>
```

Two additional interfaces exist that are used to communicate with the access-point module: wlan-ap0 and wlan-GigabitEthernet0. You must configure the wlan-ap0 interface with an IP address (any private IP address works; check RFC 1918 for available private subnets) in order to allow reverse Telnet from the router to the access-point module:

```
interface wlan-ap0
 description Service module interface to manage the embedded AP
 ip address <wlanap0-ip-address> 255.255.255.255
 arp timeout 0
```

As mentioned earlier, one advantage of having the access-point module is that it can be deployed in both modes: autonomous (standalone), and lightweight (unified). In lightweight mode, the access point associates with a WLAN controller and downloads its configuration file from there. Thus you must do all necessary configuration for secure wireless access on the controller. In autonomous mode, the configuration is entered on the access point itself, without using a WLAN controller in the middle. The following command is used on the router to define the mode of operation of the access point:

`service-module wlan-ap 0 bootimage autonomous`, for autonomous mode

`service-module wlan-ap 0 bootimage unified`, for lightweight mode

Autonomous Mode

Configure the wlan-GigabitEthernet0 interface as a trunk in order to allow traffic from multiple VLANs to pass onto the access point:

```
interface Wlan-GigabitEthernet0
 description Internal switch interface connecting to the embedded AP
 switchport mode trunk
 switchport trunk native vlan 10
```

Just as for the Cisco 871W, you must configure an AAA server for EAP authentication, as well as the desired SSIDs to be used on the radio interface:

```
!!AAA server configuration!!
  aaa new-model
  aaa group server radius <aaa-group-name>
   server-private <aaa-server-address> auth-port 1812 acct-port 1813
   key 0 <server-key>
  aaa authentication login eap <list-name> group <aaa-group-name>
  aaa authorization exec default local
  ip radius source-interface BVI1
```

```
!!SSID configuration!!
dot11 ssid corporate
 vlan 10
 authentication open eap <eap-list-name>
 authentication network-eap <eap-list-name> -- !!Only if LEAP is used
 authentication key-management wpa optional

!!Dot11Radio0 interface configuration!!
 interface Dot11Radio0
  no ip address
  no ip route-cache
  encryption vlan 10 mode ciphers aes-ccm tkip wep128
  broadcast-key vlan 10 change 30
  ssid corporate
  station-role root

!!Sub-interface for bridge-group 1!!
 interface Dot11Radio0.1
  encapsulation dot1Q 10 native
  no ip route-cache
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
  bridge-group 1 spanning-disabled

!!GigabitEthernet0 interface that connects AP to router!!
 interface GigabitEthernet0
  description the embedded AP GigabitEthernet 0 is an internal
  interface connecting AP with the host router
  ip address <ip-address> <subnet-mask>
  no ip route-cache
```

Note: You can configure the GigabitEthernet0 interface with a static IP address taken from the pool configured on the router in order to be able to manage and monitor the access point.

```
!!Sub-interface for bridge-group 1!!
interface GigabitEthernet0.1
 encapsulation dot1Q 10 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
```

```
!!BVI1 interface!!
interface BVI1
 ip address dhcp client-id GigabitEthernet0
 no ip route-cache
```

Lightweight Mode

In lightweight mode, the access point associates with a WLAN controller and downloads the configuration from it. No configuration is entered on the access-point CLI. The router is configured with a DHCP pool; it acts as a DHCP server for the access point and provides it with the management IP address of the controller using option 43, as follows:

```
ip dhcp pool client
   import all
   network <subnet-address> <subnet-mask>
   domain-name cisco.com
   option 150 ip <tftpserver-address-for call manager>
   netbios-name-server <netbios-address>
   dns-server <dnsserver-address>
   default-router <vlan10-address>
   option 43 hex <hexvalue>
```

For instructions about how to derive the hex value, please refer to "Configuring DHCP Option 43 for Lightweight Access Points".

After getting the IP address of the controller, the access point contacts the controller and requests to join it using the Control and Provisioning of Wireless Access Points (CAPWAP) message exchange.

For this deployment, you should define a RADIUS server (Cisco Secure ACS) on the controller, along with WLANs (SSIDs). You should also configure the ACS with the corresponding EAP methods to be used on the defined SSIDs. For instructions about how to complete these steps, please refer to "EAP Authentication with WLAN Controllers (WLC) Configuration Example".

Monitoring the Access-Point Module

An important aspect of any solution is the monitoring capabilities that it provides. It is important for the administrator to know how the different components of the solution are performing in order to be able to react promptly to any failure in the operation.

The Cisco Prime™ Network Control System (NCS) is a powerful tool for monitoring access points and WLAN controllers. Cisco Prime NCS is useful mostly for unified (lightweight) architectures; it offers some basic monitoring features for autonomous access points.

In a unified deployment, the NCS is used to manage all the WLAN controllers. After adding a controller to it, the NCS offers services such as autodiscovery of access points that associate to that controller, autodiscovery of rogue access points, location, etc. in addition to many other features. For detailed information about the Cisco Prime NCS, please refer to Cisco Network Control System.

Guest Access

Cisco Virtual Office offers the possibility of having the spouse and kids, and any guests, connect to the Internet through the spoke router. For wired connection, Cisco Virtual Office uses 802.1x for device authentication; if no valid credentials are provided, the device is placed into a guest VLAN, and has access to the public Internet only—not the corporate network. For wireless connection, you can configure a separate guest SSID on the Cisco 871W or the access-point module on the Cisco 881W. This SSID links to a different VLAN, and the machines associated to it will be given access only to the public Internet. WEP or WPA-PSK is usually used for authentication on guest SSIDs. When WPA-PSK is used, TKIP is best for authentication. Note that at this point the administrator is required to configure the WPA or WEP key on the CLI of the router or the access point. Soon, role-based access will be supported, and the user will be given limited access to modify the WPA and WEP keys. Following are configuration samples for the Cisco 871W and the access-point module on the Cisco 881W (autonomous and lightweight) for guest access.

Cisco 871W

To configure the Cisco 871W Integrated Services Router for guest access, you must add a new VLAN as well as a bridge group, bridge-group virtual interface, radio subinterface, and an SSID. Following is the configuration of a guest SSID with WPA-PSK as the authentication method:

```
!!DHCP pool for guests!!
ip dhcp pool public
   import all
   network 10.1.1.0 255.255.255.0
   default-router 10.1.1.1
   dns-server <dnsserver-address>

!!Configuring a new BVI!!
interface BVI2
 ip address 10.1.1.1 255.255.255.0

!!New VLAN for guests-associated with bridge-group 2!!
interface Vlan20
 no ip address
 no autostate
 bridge-group 2
 bridge-group 2 spanning-disabled

!!Guest SSID!!
dot11 ssid guest
   vlan 20
   authentication open
   authentication key-management wpa
   wpa-psk ascii 0 <desired-psk>

!!Adding SSID to radio interface!!
interface Dot11Radio0
 encryption vlan 20 mode ciphers tkip
 broadcast-key vlan 20 change 30
```

```
 ssid guest

!!Radio sub-interface for bridge-group 2!!
interface Dot11Radio0.2
 description Internet access
 encapsulation dot1Q 20
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 spanning-disabled
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
```

For WEP authentication, use the same configuration, but replace the part corresponding to “SSID guest” and “interface Dot11Radio0” with the following:

```
ssid guest
 vlan 20
 authentication open
interface Dot11Radio0
 broadcast-key vlan 20 change 30
 encryption vlan 20 key 1 size 128bit 0 <desired-wepkey> transmit-key
 encryption vlan 20 mode wep mandatory
 ssid guest
```

Cisco 881W Integrated Services Router and Access-Point Module

For the Cisco 881 Integrated Services Router, the difference is that no BVI 2 interface exists. Instead, VLAN 20 (the guest VLAN) is configured as the default gateway for bridge-group 2 on the router, as follows:

```
interface Vlan20
 ip address 10.1.1.1 255.255.255.0
 ip pim sparse-dense-mode
 ip virtual-reassembly
 no autostate
```

For guest access in autonomous mode using WPA-PSK, you should configure the access-point module as such.

Note: To enable WEP authentication instead, you must make the same modifications mentioned previously to the following configuration sample (guest SSID and dot11radio interface) on the access-point module:

```
!!Sub-interface for bridge-group 1!!
interface GigabitEthernet0.2
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 2
```

```
 no bridge-group 2 source-learning
 bridge-group 2 spanning-disabled

!!Guest SSID!!
dot11 ssid guest
 vlan 20
 authentication open
 authentication key-management wpa
 guest-mode
 wpa-psk ascii 0 <desired-psk>

!!Enabling the guest SSID on the radio interface!!
interface Dot11Radio0v
 encryption vlan 20 mode ciphers tkip
 broadcast-key vlan 20 change 30
 ssid guest
!!Radio sub-interface for bridge-group 1!!
interface Dot11Radio0.2
 encapsulation dot1Q 20
 no ip route-cache
 bridge-group 2
 bridge-group 2 subscriber-loop-control
 bridge-group 2 block-unknown-source
 no bridge-group 2 source-learning
 no bridge-group 2 unicast-flooding
 bridge-group 2 spanning-disabled
```

For lightweight mode, you can configure the controller with a separate SSID for guest access, following the steps in "EAP Authentication with WLAN Controllers (WLC) Configuration Example".

Wireless Phones

Cisco Virtual Office allows the teleworkers to use wireless IP phones (for example, Cisco Unified Wireless IP Phone 7921G models) or dual-mode phones, personal digital assistants (PDAs), iPhones, etc. that support WPA-Enterprise or WPA2-Enterprise transparently through the spoke router. Wireless IP phones can authenticate using EAP-FAST or PEAP. These phones are authenticated with the corporate AAA and connect to the corporate Cisco Unified Communications Manager using the secure tunnel established between the spoke router and the hub at the headend. For more information about support of VoIP over wireless and dual-mode phones with Cisco Virtual Office, please refer to the "Cisco Virtual Office - Secure Voice and Video" guide at http://www.cisco.com/go/cvo.

Wireless Printers

Cisco Virtual Office supports wireless printers. Typically, printers are placed on the guest VLAN and thus considered part of the Internet. Both teleworkers and guests are allowed to print when Split Tunneling is enabled. In that case, the corporate traffic would be going through the VPN tunnel while other traffic goes straight to the Internet. The administrator can also enable advanced layered security services and apply zone-based firewall for a more thorough control of domain isolation and domain sharing functions: the printer would be in the "untrusted" zone and the teleworkers in the "trusted" zone, with traffic being allowed from the trusted to the untrusted zone

accordingly. For more information about zone-based firewall configuration, please refer to the “Cisco Virtual Office-Advanced Layered Security” guide at http://www.cisco.com/go/cvo.

Notes

It should be noted that upgrading a Mac OS may cause some problems with wireless access. Problems occurred when upgrading Tiger (MAC OS X v10.4) to Leopard (MAC OS X v10.5) and using EAP methods. Changing to WPA solved that problem.

Also note that, by default, the spoke Cisco 871W router and the access-point module on the Cisco 881W spoke router, when in autonomous mode, looks for the least-congested wireless channel upon bootup, and assigns the user to it. This channel, however, will not change until the router is reloaded, even if heavy interference is faced later on. Thus, if you have interference with wireless access, you should reload the router so it can find a new, better channel to associate to. For the Cisco 881W access-point module in lightweight mode, however, the controller automatically assigns the best channel by autoscanning the wireless environment.

Troubleshooting Wireless Connectivity Problems

Useful Show and Debug Commands

- **show dot11 associations** displays the devices that are wirelessly connecting to the router and the corresponding SSIDs they associate to.
- **show dot11 statistics interface** displays statistics about packets sent and received on the Dot11Radio interface.
- **show controllers dot11radio 0** displays information about the radio interface, including the wireless channel being used.
- **debug dot11 events** displays log messages of wireless events (for example, reception and transmission of packets) as they happen.
- **debug dot11 station connection failure** displays logs when stations fail to associate or authenticate.

Tips for Getting a Good Wireless Signal

In order to get a wireless signal at a good strength, you should do the following:

- Place the router in a central location, away from walls and elevated from the ground.
- Place the router away from any metal objects.
- Adjust the position of directional antennae to get the best possible signal where you are located.
- To expand the wireless coverage at the remote location, you can use different antennae with higher gain.

References

- Cisco Virtual Office: http://www.cisco.com/go/cvo
- Configuring DHCP Option 43 for Lightweight Access Points: http://www.cisco.com/en/US/docs/wireless/access_point/1100/installation/guide/110h_f.html
- EAP Authentication with WLAN Controllers (WLCs) configuration example: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a0080665d18.shtml

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C07-682984-00 08/11