Deploying IEEE 802.1x Technology with Cisco Integrated Services Routers

Abstract

This document discusses the support, application, and deployment scenarios of IEEE 802.1x features for Cisco® integrated services routers. It covers 802.1x authentication for wired networks only.

Introduction

Cisco integrated services routers support a comprehensive array of services and solutions addressing the needs of voice, video, wireless, and data applications for enterprise branch offices, small and medium-sized businesses (SMBs), and small offices or home offices (SOHOs).

The 802.1x standard is an IEEE standard for media-level access control, offering the capability to permit or deny network connectivity, control VLAN access, and apply traffic policy based on user or machine identity.

Identify Based Networking Services (IBNS) is a technology solution that provides the tools to improve the security of physical and logical access to LANs. IBNS incorporates all the capabilities defined in the IEEE 802.1x standard and provides enhancements and extensions for improving identity-based access control.

IEEE 802.1x Support on Cisco Integrated Services Routers

Cisco integrated services routers can greatly benefit from the IEEE 802.1x and IBNS features to improve security and simplify configurations in the field. Table 1 summarizes the IEEE 802.1x features currently supported by the integrated services routers with the various switch hardware options. Cisco IOS® Software Release 12.4(11)T is required for the 802.1x features on the integrated services router platforms. Please note that the Cisco EtherSwitch® Service Modules have 802.1x feature parity with the Cisco Catalyst® 3750 Switches running the same Cisco IOS Software releases as the Cisco Catalyst 3750.

Table 1. IEEE 802.1x Support on Cisco Integrated Services Routers

Feature	Cisco 870 Series	Cisco 1800 Fixed Configuration	Cisco 1841 and Cisco 2800 and 3800 Series with HWIC-4ESW, HWICD-9ESW, or Cisco EtherSwitch Network Modules
802.1x Basic Authentication	Yes	Yes	Yes
802.1x with Port Security	No	Yes*	Yes*
802.1x with Voice VLAN ID (VVID)	Yes	Yes	Yes
802.1x with VLAN Assignment	Yes	Yes	Yes
802.1x with Spouse and Kids on Layer 3 Fast Ethernet Port	–	Yes	Yes

Feature	Cisco 870 Series	Cisco 1800 Fixed Configuration	Cisco 1841 and Cisco 2800 and 3800 Series with HWIC-4ESW, HWICD-9ESW, or Cisco EtherSwitch Network Modules
802.1x with Spouse and Kids on Switch Virtual Interface (SVI)	Yes	N/A	N/A
802.1x with Guest VLAN	Yes	Yes	Yes
Authentication Fail VLAN**	No (works only with single host mode)	Yes	Yes
802.1x Single-Host Mode	No	Yes	Yes
802.1x Multi-Host Mode	Yes	Yes	Yes
802.1x MIB: Cisco PAE MIB and IEEE PAE MIB	Yes	Yes	Yes
802.1x with Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)	Yes	Yes	Yes
802.1x with EAP-Message Digest Algorithm 5 (EAP-MD5)	Yes	Yes	Yes
802.1x with EAP-Transparent LAN Services (EAP-TLS)	Yes	Yes	Yes
MAC Authentication Bypass	Layer 3 only	Layer 3 only	Layer 3 only

* 802.1x with Port Security with this hardware option works differently compared to the Cisco Catalyst 3000 and Catalyst 4000 switches. A port with this hardware option is secured after it is authorized, when it is configured for single host mode. The command-line interface (CLI) “802.1x Port Security” is not supported.
** Known caveats associated with Authentication Fail VLAN are documented with CSCsj80588, CSCsj51624, and CSCsj55636.

IEEE 802.1x Applications with Cisco Integrated Services Routers

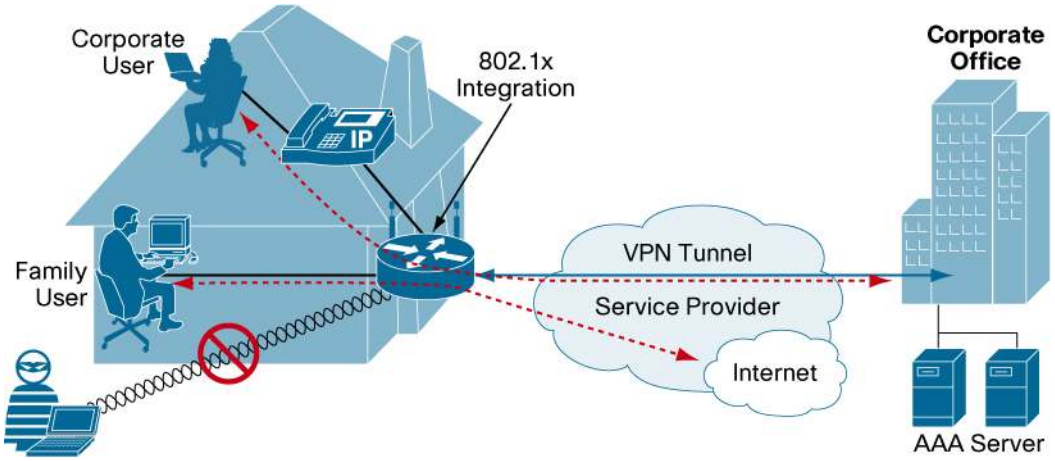
Enterprise Class Teleworker: VPN Access Control Using 802.1x Authentication

Enterprises increasingly rely on home offices for connectivity of day extenders, part-time teleworkers, and full-time teleworkers. In order for these workers to be optimally productive, they must have access to the same services used at the corporate site, including data, e-mail, collaboration tools, and voice and video services.

The home access router provides connectivity to the corporate network through a VPN tunnel through the Internet. In the home LAN, apart from the employee, other members of the household may also be using the same access router. The VPN Access Control Using 802.1x Authentication feature allows enterprise employees to access their enterprise networks from home while allowing other household members to access only the Internet. The feature uses the IEEE 802.1x protocol framework to achieve the VPN access control. The authenticated employee has access to the VPN tunnel and unauthenticated users on the same LAN have access only to the Internet.

Figure 1 is an example of the Cisco 870 Series Router in an enterprise-class telecommuting deployment scenario, using the VPN Access Control Using 802.1x Authentication feature.

Figure 1. VPN Access Control Using 802.1x



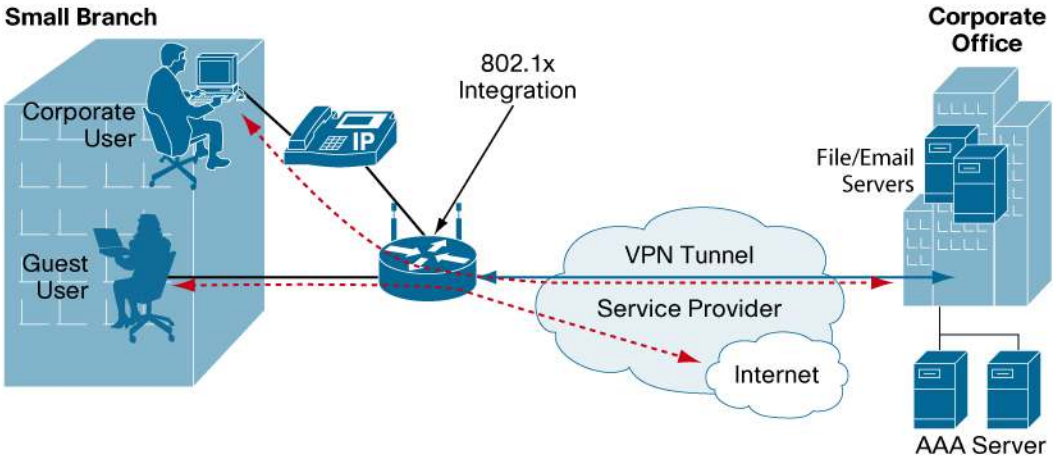
- Teleworker has separate network with VPN and Internet access
- Family user has only Internet access
- IEEE 802.1x authentication can be tied to Windows login and cached
- RADIUS server is required at enterprise main office for authentication
- Unauthorized wireless users cannot access enterprise

Enterprise Branch Office: 802.1x Guest VLAN

Many enterprises are starting to deploy 802.1x in their networks to reduce the administrative overhead associated with the demand for network connectivity outside of the typical office and cube work areas. The use of 802.1x brings the capability of dynamic assignment of a switch port to a VLAN based on the identity of the user connecting to the network. The same wired port located in an enterprise public area can be used to provide both internal access to the employees and Internet access to visitors, overcoming the static mapping limitation in traditional Layer 2 networks.

IEEE 802.1x Guest VLAN is intended for deployment in conference rooms, building lobbies, and other areas where visitors frequently require network access. It is deployed to provide Internet access to users not equipped with an 802.1x supplicant on their machine and hence not able to reply to the identity request messages received from the switch. In addition, Guest VLAN can be used for other devices such as printers that are not 802.1x-enabled. Figure 2 illustrates the deployment of a Cisco integrated services router at an enterprise branch office using the 802.1x Guest VLAN feature.

Figure 2. IEEE 802.1x Guest VLAN [[edits: File or E-Mail Servers]]



- Corporate user has separate network with access to corporate resources
- Guest user has only Internet access
- RADIUS server is required at enterprise main office for authentication

Enterprise Branch Office: IEEE 802.1x VLAN Assignment

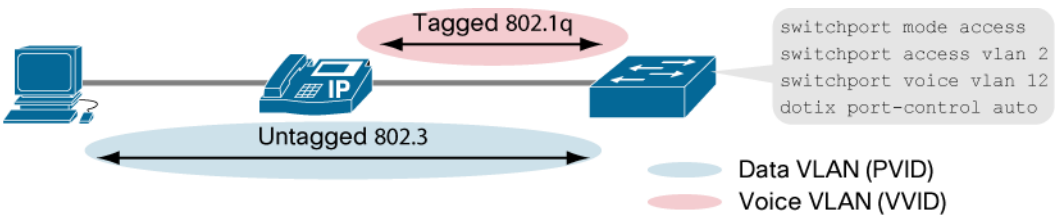
With 802.1x VLAN Assignment support, Cisco integrated services routers can dynamically assign users and devices at the enterprise branch location to the appropriate VLAN, reducing administrative overhead and eliminating physical connectivity errors.

Dynamic VLAN Assignment can be used to limit network access for certain users. With the VLAN assignment, 802.1x-authenticated ports are assigned to a VLAN based on the username of the client connected to that port. The RADIUS server database maintains the username-to-VLAN mappings. After successful 802.1x authentication of the port, the RADIUS server sends the VLAN assignment to the switch. When the 802.1x client disconnects, the assigned VLAN is reverted back to the original configured VLAN or the default VLAN if nothing is configured before.

Enterprise Branch Office and Teleworker: IEEE 802.1x with VVID

IP telephony is now an integral part of many enterprise networks. The 802.1x standard with VVID allows IP phones to use VVID for voice traffic, regardless of the authorization state of the switchport. This feature also allows the phones to work independently of IEEE 802.1x authentication, an especially useful feature with IP phones that do not support 802.1x supplicant. Figure 3 illustrates the use of VVID with 802.1x.

Figure 3. IEEE 802.1x with VVID



Conclusion

With switching capabilities integrated into the Cisco integrated services routers, 802.1x and IBNS solutions are critical to ensure network access control with user and device authentication, and to provide policy management and enforcement for the authenticated users and devices. This document provided information about 802.1x application and support on integrated services routers for customers evaluating IBNS support for their network.

For More Information

- Cisco integrated services routers: http://www.cisco.com/go/isr
- Cisco IOS Software Release 12.4(11)T release notes with 802.1x feature support: http://www.cisco.com/en/US/partner/products/ps6441/prod_release_note09186a00804a19ae.html#wp1820211
- Deploying 802.1x-based port authentication on the Cisco Enterprise Class Teleworker solution (with configuration examples): http://www/en/US/products/ps6660/products_white_paper0900aecd805a5ab5.shtml
- Cisco EtherSwitch Modules comparison: http://www.cisco.com/en/US/products/ps5854/products_qanda_item0900aecd802a9470.shtml

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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

C11-428590-00 9/07