IEEE 802.1X

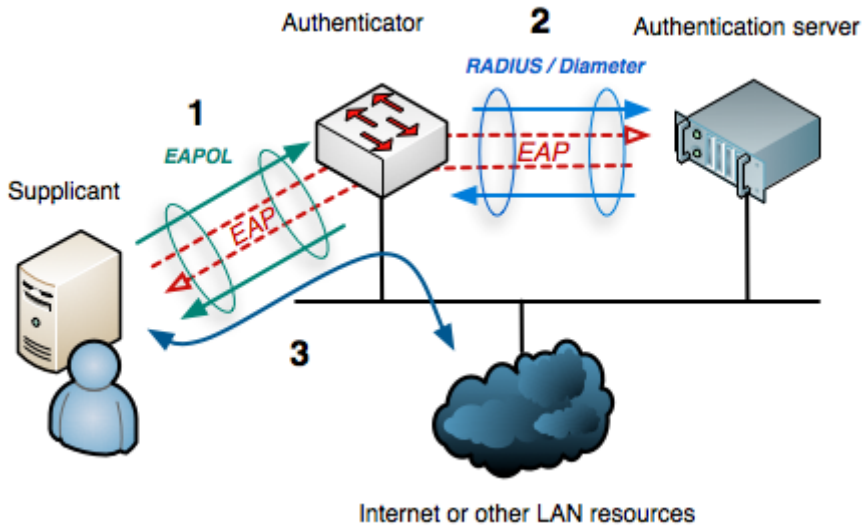
IEEE 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over wired IEEE 802 networks[1] and over 802.11 wireless networks,[2] which is known as "EAP over LAN" or EAPOL.[3] EAPOL was originally specified for IEEE 802.3 Ethernet, IEEE 802.5 Token Ring, and FDDI (ANSI X3T9.5/X3T12 and ISO 9314) in 802.1X-2001,[4] but was extended to suit other IEEE 802 LAN technologies such as IEEE 802.11 wireless in 802.1X-2004.[5] The EAPOL was also modified for use with IEEE 802.1AE ("MACsec") and IEEE 802.1AR (Secure Device Identity, DevID) in 802.1X-2010[6][7] to support service identification and optional point to point encryption over the internal LAN segment.

Contents

Overview

802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The **supplicant** is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The **authenticator** is a network device that provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point; and the **authentication server** is typically a trusted server that can receive and respond to requests for network access, and can tell the authenticator if the connection is to be allowed, and various settings that should apply to that client's connection or setting. Authentication servers typically run software supporting the RADIUS and EAP protocols. In some cases, the authentication server software may be running on the authenticator hardware.



EAP data is first encapsulated in EAPOL frames between the Supplicant and Authenticator, then re-encapsulated between the Authenticator and the Authentication server using RADIUS or Diameter.

The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant must initially provide the required credentials to the authenticator - these will have been specified in advance by the network administrator and could include a user name/password or a permitted digital certificate. The authenticator forwards these credentials to the authentication server to decide whether access is to be granted. If the authentication server determines the credentials are valid, it informs the authenticator, which in turn allows the supplicant (client device) to access resources located on the protected side of the network.[8]

Protocol operation

EAPOL operates over the data link layer, and in Ethernet II framing protocol has an EtherType value of 0x888E.

Port entities

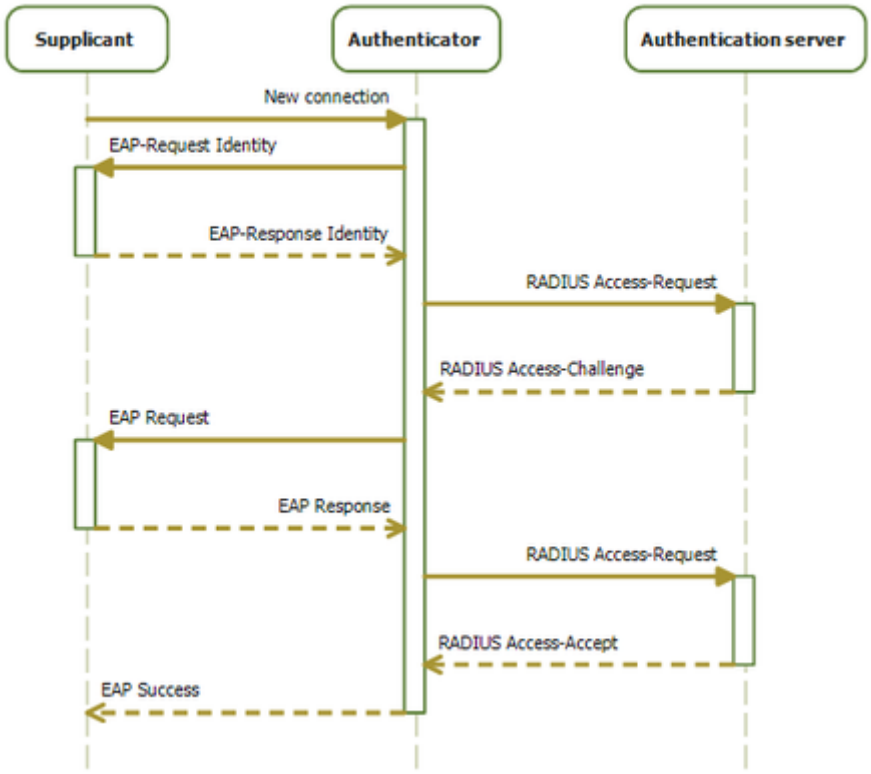
802.1X-2001 defines two logical port entities for an authenticated port—the "controlled port" and the "uncontrolled port". The controlled port is manipulated by the 802.1X PAE (Port Access Entity) to allow (in the authorized state) or prevent (in the unauthorized state) network traffic ingress and egress to/from the controlled port. The uncontrolled port is used by the 802.1X PAE to transmit and receive EAPOL frames.

802.1X-2004 defines the equivalent port entities for the supplicant; so a supplicant implementing 802.1X-2004 may prevent higher-level protocols from being used if it is not content that authentication has successfully completed. This is particularly useful when an EAP method providing mutual authentication is used, as the supplicant can prevent data leakage when connected to an unauthorized network.

Typical authentication progression

The typical authentication procedure consists of:

1. **Initialization** On detection of a new supplicant, the port on the switch (authenticator) is enabled and set to the "unauthorized" state. In this state, only 802.1X traffic is allowed; other traffic, such as the Internet Protocol (and with that TCP and UDP), is dropped.



Sequence diagram of the 802.1X progression

2. **Initiation** To initiate authentication the authenticator will periodically transmit EAP-Request Identity frames to a special Layer 2 address (01:80:C2:00:00:03) on the local network segment. The supplicant listens on this address, and on receipt of the EAP-Request Identity frame, it responds with an EAP-Response Identity frame containing an identifier for the supplicant such as a User ID. The authenticator then encapsulates this Identity response in a RADIUS Access-Request packet and forwards it on to the authentication server. The supplicant may also initiate or restart authentication by sending an EAPOL-Start frame to the authenticator, which will then reply with an EAP-Request Identity frame.
3. **Negotiation** *(Technically EAP negotiation)* The authentication server sends a reply (encapsulated in a RADIUS Access-Challenge packet) to the authenticator, containing an EAP Request specifying the EAP Method (The type of EAP based authentication it wishes the supplicant to perform). The authenticator encapsulates the EAP Request in an EAPOL frame and transmits it to the supplicant. At this point, the supplicant can start using the requested EAP Method, or do a NAK ("Negative Acknowledgement") and respond with the EAP Methods it is willing to perform.
4. **Authentication** If the authentication server and supplicant agree on an EAP Method, EAP Requests and Responses are sent between the supplicant and the authentication server (translated by the authenticator) until the authentication server responds with either an EAP-Success message (encapsulated in a RADIUS Access-Accept packet), or an EAP-Failure message (encapsulated in a RADIUS Access-Reject packet). If authentication is successful, the authenticator sets the port to the "authorized" state and normal traffic is allowed, if it is unsuccessful the port remains in the "unauthorized" state. When the supplicant logs off, it sends an EAPOL-logoff message to the authenticator, the authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic.

Implementations

An open-source project known as Open1X produces a client, Xsupplicant. This client is currently available for both Linux and Windows. The main drawbacks of the Open1X client are that it does not provide comprehensible and extensive user documentation and the fact that most Linux vendors do not provide a package for it. The more general wpa_supplicant can be used for 802.11 wireless networks and wired networks. Both support a very wide range of EAP types.[9]

The iPhone and iPod Touch support 802.1X as of the release of iOS 2.0. Android has support for 802.1X since the release of 1.6 Donut. Chrome OS has supported 802.1X since mid-2011.[10]

macOS has offered native support since 10.3.[11]

Avenda Systems provides a supplicant for Windows, Linux and macOS. They also have a plugin for the Microsoft NAP framework.[12] Avenda also offers health checking agents.

Windows

Windows defaults to not responding to 802.1X authentication requests for 20 minutes after a failed authentication. This can cause significant disruption to clients.

The block period can be configured using the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\dot3svc\BlockTime[13] DWORD value (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\wlansvc\BlockTime for wireless networks) in the registry (entered in minutes). A hotfix is required for Windows XP SP3 and Windows Vista SP2 to make the period configurable.[14]

Wildcard server certificates are not supported by EAPHost, the Windows component that provides EAP support in the operating system.[15] The implication of this is that when using a commercial certification authority, individual certificates must be purchased.

Windows XP

Windows XP has major issues with its handling of IP address changes that result from user-based 802.1X authentication that changes the VLAN and thus subnet of clients.[16] Microsoft has stated that it will not backport the SSO feature from Vista that resolves these issues.[17]

If users are not logging in with roaming profiles, a hotfix must be downloaded and installed if authenticating via PEAP with PEAP-MSCHAPv2.[18]

Windows Vista

Windows Vista-based computers that are connected via an IP phone may not authenticate as expected and, as a result, the client can be placed into the wrong VLAN. A hotfix is available to correct this.[19]

Windows 7

Windows 7 based computers that are connected via an IP phone may not authenticate as expected and, as a result, the client can be placed into the wrong VLAN. A hotfix is available to correct this.[19]

Windows 7 does not respond to 802.1X authentication requests after initial 802.1X authentication fails. This can cause significant disruption to clients. A hotfix is available to correct this.[20]

Windows PE

For most enterprises deploying and rolling out operating systems remotely, it is worth noting that Windows PE does not have native support for 802.1X. However, support can be added to WinPE 2.1[21] and WinPE 3.0[22] through hotfixes that are available from Microsoft. Although full documentation is not yet available, preliminary documentation for the use of these hotfixes is available via a Microsoft blog.[23]

Linux

Most Linux distributions support 802.1X via wpa_supplicant and desktop integration like NetworkManager.

Federations

eduroam (the international roaming service), mandates the use of 802.1X authentication when providing network access to guests visiting from other eduroam enabled institutions.[24]

BT (British Telecom, PLC) employs Identity Federation for authentication in services delivered to a wide variety of industries and governments.[25]

Proprietary extensions

MAB (MAC Authentication Bypass)

Not all devices support 802.1X authentication. Examples include network printers, Ethernet-based electronics like environmental sensors, cameras, and wireless phones. For those devices to be used in a protected network environment, alternative mechanisms must be provided to authenticate them.

One option would be to disable 802.1X on that port, but that leaves that port unprotected and open for abuse. Another, slightly more reliable option is to use the MAB option. When MAB is configured on a port, that port will first try to check if the connected device is 802.1X compliant, and if no reaction is received from the connected device, it will try to authenticate with the AAA server using the connected device's MAC address as username and password. The network administrator then must make provisions on the RADIUS server to authenticate those MAC-addresses, either by adding them as regular users or implementing additional logic to resolve them in a network inventory database.

Many managed Ethernet switches[26] offer options for this.

Vulnerabilities in 802.1X-2001 and 802.1X-2004

Shared media

In the summer of 2005, Microsoft's Steve Riley posted an article (based on the original research of Microsoft MVP Svyatoslav Pidgorny) detailing a serious vulnerability in the 802.1X protocol, involving a man in the middle attack. In summary, the flaw stems from the fact that 802.1X authenticates only at the beginning of the connection, but after that authentication, it's possible for an attacker to use the

authenticated port if he has the ability to physically insert himself (perhaps using a workgroup hub) between the authenticated computer and the port. Riley suggests that for wired networks the use of IPsec or a combination of IPsec and 802.1X would be more secure.[27]

EAPOL-Logoff frames transmitted by the 802.1X supplicant are sent in the clear and contain no data derived from the credential exchange that initially authenticated the client.[28] They are therefore trivially easy to spoof on shared media and can be used as part of a targeted DoS on both wired and wireless LANs. In an EAPOL-Logoff attack a malicious third party, with access to the medium the authenticator is attached to, repeatedly sends forged EAPOL-Logoff frames from the target device's MAC Address. The authenticator (believing that the targeted device wishes to end its authentication session) closes the target's authentication session, blocking traffic ingressing from the target, denying it access to the network.

The 802.1X-2010 specification, which began as 802.1af, addresses vulnerabilities in previous 802.1X specifications, by using MACSec IEEE 802.1AE to encrypt data between logical ports (running on top of a physical port) and IEEE 802.1AR (Secure Device Identity / DevID) authenticated devices.[6][7][29][30]

As a stopgap, until these enhancements are widely implemented, some vendors have extended the 802.1X-2001 and 802.1X-2004 protocol, allowing multiple concurrent authentication sessions to occur on a single port. While this prevents traffic from devices with unauthenticated MAC addresses ingressing on an 802.1X authenticated port, it will not stop a malicious device snooping on traffic from an authenticated device and provides no protection against MAC spoofing, or EAPOL-Logoff attacks.

Alternatives

The IETF-backed alternative is the Protocol for Carrying Authentication for Network Access (PANA), which also carries EAP, although it works at layer 3, using UDP, thus not being tied to the 802 infrastructure.[31]

See also

- AEGIS SecureConnect
- IEEE 802.11i-2004

References

1. "EAP Usage Within IEEE 802" (https://datatracker.ietf.org/doc/html/rfc3748#section-3.3). *Extensible Authentication Protocol (EAP)* (https://datatracker.ietf.org/doc/html/rfc3748). sec. 3.3. doi:10.17487/RFC3748 (https://doi.org/10.17487%2FRFC3748). RFC 3748 (https://datatracker.ietf.org/doc/html/rfc3748).
2. "Link Layer" (https://datatracker.ietf.org/doc/html/rfc3748#section-7.12). *Extensible Authentication Protocol (EAP)* (https://datatracker.ietf.org/doc/html/rfc3748). sec. 7.12. doi:10.17487/RFC3748 (https://doi.org/10.17487%2FRFC3748). RFC 3748 (https://datatracker.ietf.org/doc/html/rfc3748).
3. IEEE 802.1X-2001, § 7
4. IEEE 802.1X-2001, § 7.1 and 7.2
5. IEEE 802.1X-2004, § 7.6.4
6. IEEE 802.1X-2010, page iv
7. IEEE 802.1X-2010, § 5

8. "802.1X Port-Based Authentication Concepts" (https://web.archive.org/web/20121014224422/http://www.wireless-nets.com/resources/downloads/802.1x_C2.html). Archived from the original (http://www.wireless-nets.com/resources/downloads/802.1x_C2.html) on 2012-10-14. Retrieved 2008-07-30.
9. "eap_testing.txt from wpa_supplicant" (https://w1.fi/cgit/hostap/plain/wpa_supplicant/eap_testing.txt). Retrieved 2010-02-10.
10. Sheth, Rajen (August 10, 2011). "The computer that keeps getting better" (https://cloud.googleblog.com/2011/08/the-computer-that-keeps-getting-better.html). *Google Cloud Official Blog*. Retrieved 2022-07-02.
11. Negrino, Tom; Smith, Dori (2003). *Mac OS X Unwired: A Guide for Home, Office, and the Road* (https://books.google.com/books?id=Tdr5DIxmQYgC&pg=PA19). O'Reilly Media. p. 19. ISBN 978-0596005085. Retrieved 2022-07-02.
12. "NAP clients for Linux and Macintosh are available" (https://docs.microsoft.com/en-us/archive/blogs/nap/nap-clients-for-linux-and-macintosh-are-available). *Network Access Protection (NAP) team blog*. 2008-12-16.
13. "20 minute delay deploying Windows 7 on 802.1x? Fix it here!" (https://docs.microsoft.com/en-us/archive/blogs/jeff_stokes/20-minute-delay-deploying-windows-7-on-802-1x-fix-it-here). *Dude where's my PFE? blog*. 2013-01-24.
14. "A Windows XP-based, Windows Vista-based or Windows Server 2008-based computer does not respond to 802.1X authentication requests for 20 minutes after a failed authentication" (https://support.microsoft.com/en-us/topic/a-windows-xp-based-windows-vista-based-or-windows-server-2008-based-computer-does-not-respond-to-802-1x-authentication-requests-for-20-minutes-after-a-failed-authentication-8fcef6e5-4526-17db-e430-22f1f51a84ad). *Microsoft Support*. 2009-09-17. Retrieved 2022-07-03.
15. "EAPHost in Windows Vista and Longhorn (January 18, 2006)" (https://docs.microsoft.com/en-us/previous-versions/cc730460(v=msdn.10)?redirectedfrom=MSDN). *Microsoft Docs*. 2007-01-18. Retrieved 2022-07-03.
16. "You experience problems when you try to obtain Group Policy objects, roaming profiles, and logon scripts from a Windows Server 2003-based domain controller" (https://web.archive.org/web/20080422000723/http://support.microsoft.com/kb/935638). *Microsoft Support*. 2007-09-14. Archived from the original (http://support.microsoft.com/kb/935638) on 2008-04-22. Retrieved 2010-02-10.
17. "802.1x with dynamic vlan switching - Problems with Roaming Profiles" (https://web.archive.org/web/20110824194607/http://social.technet.microsoft.com/forums/en-US/winserverNAP/thread/f68dc3f0-744a-4d0f-b85a-87f8bc531fd0/). *Microsoft TechNet Forums*. Archived from the original (http://social.technet.microsoft.com/forums/en-US/winserverNAP/thread/f68dc3f0-744a-4d0f-b85a-87f8bc531fd0/) on 2011-08-24. Retrieved 2010-02-10. "With Vista, this is not a problem at all with the SSO feature, however, this feature does not exist in XP and unfortunately, we do not have any plans to backport this feature to XP as it is just too complex a change."
18. "A Windows XP Service Pack 3-based client computer cannot use the IEEE 802.1X authentication when you use PEAP with PEAP-MSCHAPv2 in a domain" (https://web.archive.org/web/20100316162915/http://support.microsoft.com/kb/969111). *Microsoft support*. 2009-04-23. Archived from the original (http://support.microsoft.com/kb/969111) on 2010-03-16. Retrieved 2010-03-23.
19. "A computer that is connected to an IEEE 802.1X authenticated network through a VOIP phone does not connect to the correct network after you resume it from Hibernate mode or Sleep mode" (https://support.microsoft.com/en-us/topic/a-computer-that-is-connected-to-an-ieee-802-1x-authenticated-network-via-another-802-1x-enabled-device-does-not-connect-to-the-correct-network-1ab27ed2-3ccb-fc02-19d2-5fb36b4c0bf2). *Microsoft Support*. 2010-02-08. Retrieved 2022-07-03.

20. "No response to 802.1X authentication requests after authentication fails on a computer that is running Windows 7 or Windows Server 2008 R2" (https://web.archive.org/web/20101114001734/http://support.microsoft.com/kb/980295). *Microsoft Support*. 2010-03-08. Archived from the original (http://support.microsoft.com/kb/980295) on 2010-11-14. Retrieved 2010-03-23.
21. "Windows PE 2.1 does not support the IEEE 802.1X authentication protocol" (https://web.archive.org/web/20100305170820/http://support.microsoft.com/kb/975483). *Microsoft Support*. 2009-12-08. Archived from the original (http://support.microsoft.com/kb/975483) on 2010-03-05. Retrieved 2010-02-10.
22. "The IEEE 802.1X authentication protocol is not supported in Windows Preinstall Environment (PE) 3.0" (https://support.microsoft.com/en-us/topic/the-ieee-802-1x-authentication-protocol-is-not-supported-in-windows-preinstall-environment-pe-3-0-a3f0be1d-e688-4925-53ef-49a4139aae3a). *Microsoft Support*. 2009-12-08. Retrieved 2022-07-03.
23. "Adding Support for 802.1X to WinPE" (https://web.archive.org/web/20110617114548/http://blogs.technet.com/b/deploymentguys/archive/2010/03/02/adding-support-for-802-1x-to-winpe.aspx). *The Deployment Guys blog*. 2010-03-02. Archived from the original (http://blogs.technet.com/deploymentguys/archive/2010/03/02/adding-support-for-802-1x-to-winpe.aspx) on 2011-06-17. Retrieved 2010-03-03.
24. "How does eduroam work?" (https://eduroam.org/how/). *eduroam*. Retrieved 2022-07-03.
25. "BT Identity and Access Management" (https://web.archive.org/web/20110613160018/http://www.ca.com/files/SuccessStories/bt_ss_165270.pdf) (PDF). Archived from the original (http://www.ca.com/files/SuccessStories/bt_ss_165270.pdf) (PDF) on 2011-06-13. Retrieved 2010-08-17.
26. "Dell PowerConnect 6200 series CLI Guide" (https://web.archive.org/web/20121118212447/http://support.dell.com/support/edocs/network/PC62xx/en/CLI/PDF/cli_en.pdf) (PDF). p. 622, Revision: A06-March 2011. Archived from the original (http://support.dell.com/support/edocs/network/pc62xx/en/CLI/PDF/cli_en.pdf) (PDF) on 2012-11-18. Retrieved 26 January 2013.
27. Riley, Steve (2005-08-09). "Mitigating the Threats of Rogue Machines—802.1X or IPsec?" (https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc512611(v=technet.10)). *Microsoft Docs*. Retrieved 2022-07-03.
28. IEEE 802.1X-2001, § 7.1
29. "2 February 2010 Early Consideration Approvals" (https://web.archive.org/web/20100706171048/http://standards.ieee.org/board/rev/110early.html). Standards.ieee.org. Archived from the original (http://standards.ieee.org/board/rev/110early.html) on 2010-07-06. Retrieved 2010-02-10.
30. "IEEE 802.1: 802.1X-2010 - Revision of 802.1X-2004" (https://web.archive.org/web/20100304232216/http://www.ieee802.org/1/pages/802.1x-2010.html). Ieee802.org. 2010-01-21. Archived from the original (http://www.ieee802.org/1/pages/802.1x-2010.html) on 2010-03-04. Retrieved 2010-02-10.
31. Philip Golden; Hervé Dedieu; Krista S. Jacobsen (2007). *Implementation and Applications of DSL Technology* (https://books.google.com/books?id=Jjkd74jY47oC&pg=PA483). Taylor & Francis. pp. 483–484. ISBN 978-1-4200-1307-8.

External links

- IEEE page on 802.1X (https://1.ieee802.org/security/802-1x/)
- GetIEEE802 Download 802.1X-2020 (https://ieeexplore.ieee.org/document/9018454)
- GetIEEE802 Download 802.1X-2010 (http://standards.ieee.org/getieee802/download/802.1X-2010.pdf)

- GetIEEE802 Download 802.1X-2004 (http://standards.ieee.org/getieee802/download/802.1X-2004.pdf)
- GetIEEE802 Download 802.1X-2001 (http://standards.ieee.org/getieee802/download/802.1X-2001.pdf)
- Ultimate wireless security guide: Self-signed certificates for your RADIUS server (https://www.techrepublic.com/article/ultimate-wireless-security-guide-self-signed-certificates-for-your-radius-server/6148560)
- WIRE1x (http://wire.cs.nctu.edu.tw/wire1x/)
- Wired Networking with 802.1X Authentication (https://technet.microsoft.com/en-us/network/bb545365.aspx) on Microsoft TechNet

---