**802.1x on Switches**

Download this File as PDF

### Content

- About this paper
- About EAP
- Client and Server Configuration
- 802.1X Configuration Limitation
- Switch Configuration
- VLANs
- Things to check with Microsoft
  - Windows 2000 and XP additional Registry Entry
  - XP patches
  - Windows 2000 patches
- Show Commands
- Troubleshooting hints
- IEEE
- Lab Config
- FAQ
- MS Case SRQ031001601501 summary

### About this paper

It is an add on to "How-To Configure PEAP implementation supported by ACS 3.2" covering also Switches. Based on lab tests done by Benjamin Basler bbasler@cisco.com and Fabi Riesen fabi@cisco.com. It is NOT an official Cisco Document.

### About EAP

EAP typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.):

![Client and Switch Talk 802.1x Switch Speaks to Auth Server Using RADIUS](image)

**Actual Authentication Conversation Is between Client and Auth Server Using EAP; the Switch Is Just a Middleman, but Is Aware of What’s Going on**

### Different EAPOL Frame Types

- EAPOL-Start
- EAPOL-Logoff
- EAP-Packet
- EAPOL-Key
- EAPOL-Encapsulated-ASF-Alert

### Booting Process in Windows:

![Boot Process](image)

### Client and Server Configuration

Basically config of client and AAA server is exactly the same like for Wireless authentication. See "How-To Configure PEAP implementation supported by ACS 3.2" We've tested PEAP-MS-CHAPv2 w/o Machine Authentication.

Current Prevalent Authentication Methods are:

- EAP-MD5: Uses MD5 based Challenge-Response for authentication
- EAP-TLS: Uses x.509 v3 PKI certificates and the TLS mechanism for authentication

[http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html](http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html)
- PEAP: Protected EAP tunnel mode EAP encapsulator. Tunnels other EAP types in an encrypted tunnel—much like web-based SSL.
- EAP-TTLS: Other EAP methods over an extended EAP-TLS encrypted tunnel.
- LEAP: Uses username/password authentication
- EAP-GTC: Generic token & OTP authentication

Further possibilities are EAP-TLS w/o Machine Authentication.

Windows2k SP4 and XP SP1 with some additional registry entry and hotfixes works like a charm. See hotfixes below.

### 802.1X Configuration Limitation

The 802.1X protocol is supported on Layer 2 static-access ports, voice VLAN ports, and Layer 3 routed ports. It is NOT supported on these port types:

- **Trunk port**—If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
- **Dynamic ports**—A port in dynamic mode can negotiate with its neighbor to become a trunk port. If you try to enable 802.1X on a dynamic port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to dynamic, the port mode is not changed.
- **Dynamic-access ports**—If you try to enable 802.1X on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and 802.1X is not enabled. If you try to change an 802.1X-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.
- **EtherChannel port**—Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error message appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
- **Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports**—You can enable 802.1X on a port that is a SPAN or RSPAN destination or reflector port. However, 802.1X is disabled until the port is removed as a SPAN or RSPAN destination or reflector port. You can enable 802.1X on a SPAN or RSPAN source port.

The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

When 802.1X is enabled on a port, you cannot configure a port VLAN that is equal to a voice VLAN. The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VMPS.

### Switch Configuration

```bash
aaa new-model
aaa authentication dot1x default group radius
  !-- Enable 802.1X authentication globally on the switch
  dot1x system-auth-control
  !-- Configure the switch for user RADIUS authorization for all network-related service requests, such as per-user ACLs or VLAN assignment.
  aaa authorization network default group radius
  !-- Note To configure per-user ACLs, single-host mode must be enabled. This setting is the default.

interface XX/YY
  !-- Enable 802.1X authentication on the interface.
  dot1x port-control auto
  !-- Enable periodic re-authentication of the client, which is disabled by default.
  dot1x reauthentications
  dot1x timeout reauth-period <seconds>
  !-- Set the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535 seconds; the default is 60.
  dot1x timeout quiet-period <seconds>
  !-- Set the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. The range is 1 to 65535 seconds; the default is 30.
  dot1x timeout tx-period seconds
  !-- Set the number of times that the switch sends an EAP-request/identity frame to the client before restarting the authentication process. The range is 1 to 10; the default is 2.
  dot1x max-req count
  !-- Allow multiple hosts (clients) on an 802.1X-authorized port. Make sure that the dot1x port-control interface configuration command set is set to auto for the specified interface
  dot1x host-mode multi-host
  !-- Specify an active VLAN as an 802.1X guest VLAN. The range is 1 to 4094.
  !-- Any VLAN can be configured as an 802.1X guest VLAN except internal (routed port) VLANs, RSPAN VLANs, or voice VLANs.
  dot1x guest-vlan vlan-id

  --snip--

radius-server host {hostname | ip-address} auth-port port-number key string
```

### VLANs

#### Kind of VLANs

- VLAN a port belongs to -> switchport access vlan <vlan-id>
- Guest VLAN --> dot1x guest-vlan <vlan-id>

- Dynamic VLAN --> VLAN assigned via Radius Assign vendor-specific tunnel attributes in the RADIUS server.

**Radius VLAN format**

The RADIUS server must return these attributes to the switch

[64] Tunnel-Type = VLAN
[65] Tunnel-Medium-Type = 802
[81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

... until 3750, you can send VLAN <NUMBER> or VLAN< NAME>
above 3750, you must send VLAN <NAME>

**When configured on the switch and the RADIUS server, 802.1X with VLAN assignment has these characteristics:**

- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN because of a configuration error.
- Configuration errors could include a VLAN specified for a routed port, a malformed VLAN ID, a nonexistent or internal (routed port) VLAN ID, or attempted assignment to a voice VLAN ID.
- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If the multiple-hosts mode is enabled on an 802.1X port, all hosts are placed in the same VLAN (specified by the RADIUS server) as the first authenticated host.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN Membership Policy Server (VMPS).

**Using 802.1X with Guest VLAN**

You can configure a guest VLAN for each 802.1X port on the switch to provide limited services to clients (for example, how to download the 802.1X client). These clients might be upgrading their system for 802.1X authentication, and some hosts, such as Windows 98 systems, might not be 802.1X-capable.

- Guest clients do NOT have an 802.1x supplicant.
- This type of guest access is provided by the switch.
- If client does not respond to 802.1x auth requests before timeout, guest access will be applied.
- Default timeout is 30 seconds with 3 retrans. Total timeout period is 90 secs by default.

When the authentication server does not receive a response to its EAPOL request/identity frame, clients that are not 802.1X-capable are put into the guest VLAN for the port, if one is configured. However, the server does not grant 802.1X-capable clients that fail authentication access to the network. Any number of hosts are allowed access once the switch port is moved to the guest VLAN. If an 802.1X-capable host joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the user-configured access VLAN, and authentication is restarted.

Having more than one MAC address per Switch port (e.g. Hub connected):
Configurable via: dot1x host-mode multi-host
- Only Cat6K with CatOS can handle more then one MAC with authentication connected to one Switch port
- Nevertheless if "dot1x host-mode multi-host" is configured on an other Switch (nonCat6K with CatOS), it only authenticates first MAC address and after successful authentication, it will pass the other MAC addresses. To prohibit this behavior (from allowing users connecting a HUB to the network), we must configure "switchport port-security".

**Things to check with Microsoft**

[http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP](http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP)

--------

**Windows 2000 and XP additional Registry Entry**

(otherwise it doesn't send a EAPOL-Log-off) according 8.4.3 in IEEE documentation

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EAPOL\Parameters\General\Global]
"AuthMode"=dword:00000001
"SupplicantMode"=dword:00000003

[http://www-tac.cisco.com/~fariesen/802/1x/802dot1XonSwitches_customer_version.html](http://www-tac.cisco.com/~fariesen/802/1x/802dot1XonSwitches_customer_version.html)
XP patches

60-Second to 120-Second Delay Occurs in User Authentication When You Log On to Windows XP in a Wireless Network
Description: http://support.microsoft.com/default.aspx?scid=kb;[LN];Q822725

DHCP Does Not Obtain a New Address When EAP Reauthenticates Across Access Points with IP Subnets That Differ.
Description: http://support.microsoft.com/default.aspx?scid=kb;[LN];Q822596

...those patches will be included in XP SP2.

Windows 2000 patches

Needed hotfix to get authenticaten working is Q823859
Description: <N/A> (MS internal) "EapType 26 Failed in RasEapMakeMessage and Returned 0x80004005" Error, the related KB article is 816757 "EapType 26 Failed in RasEapMakeMessage and Returned 0x80004005" Error

DHCP Does Not Obtain a New Address When EAP Reauthenticates Across Access Points with IP Subnets That Differ.
Description: http://support.microsoft.com/default.aspx?scid=kb;[LN];Q822596
Remark: On this page it is mention, that "The information in this article applies to: "Microsoft Windows XP Professional" and "Microsoft Windows XP Home Edition". However, according MS case (SRQ031001601501) and test setup it also applies to Windows 2000.

...those patches will be included in Windows SP5.

DHCP problem:

- DHCP starts once interface comes up.
- If 802.1x authentication takes too long, DHCP may time out:

802.1x Auth – Variable timeout.

DHCP – Timeout at 62 Sec.

Power Up Load NDIS drivers DHCP Setup Secure Channel to DC Present GINA (Ctrl-Alt-Del) Login

How to Address DHCP Timeout with 802.1x?

- Use Machine authentication – This allows the initial machine authentication to obtain an IP address.
- Force an IP address renewal – using a script, using a service, disconnect/reconnect interface.
- Don’t plug in Ethernet interface until you are ready to log in.

How DHCP behaves during a VLAN change

With DHCP hotfixes on Windows 2000 and XP it seems to work fine. After a VLAN change (new authentication with user belonging to different VLAN) following happens:
1. Machine tries three to get previous IP address (DHCP request) --> this takes about 10 second.
2. Then it is doing a new DHCP discovery and gets the proper IP address

More Microsoft Supplicant News

- Windows Server 2003 provides a management tool for configuring and pushing out 802.1x supplicant configuration using Domain Group Policies. (Only available in Windows Server 2003)
- Here's the latest from Microsoft on this:

 **************************************************
 We recognize the confusion in the recent flurry of fixes that we ve released and are rolling them into single rollup fix - 826942 (the one we originally listed). The hotfix that I list (826942) is inclusive of both Q826239 and 822596 as well as a number of wireless related fixes.
 Once the KB document is posted externally you may refer customers to it. We are working on making that happen this week.
 **************************************************

Show Commands

http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html

10.11.2003
**show vlan brief** -- check to which VLAN port belongs to.

```
zrhlab-3550b#sh vlan brief

VLAN Name                  Status    Ports
------- -------------------------------- --------- -------------------------------
1    default                active    Fa0/1, Fa0/13, Fa0/14, Fa0/15
1     Fa0/16, Fa0/17, Fa0/18, Fa0/19
2     Fa0/21, Fa0/22, Fa0/23, Gi0/1
2      Gi0/2
2    ACS                   active    Fa0/24
10   Cisco                 active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
10     Fa0/6, Fa0/7, Fa0/8, Fa0/9
99    Guest                active    Fa0/20
100   Machine              active
110   Gland                 active
120   Zurich               active
1002  fddi-default         act/unsup
1003  trcrf-default        act/unsup
1004  fddinet-default      act/unsup
1005  trbrf-default        act/unsup

zrhlab-3550b#
```

**show dot1x** -- show if dot1x is globally enabled

```
zrhlab-3550b#sh dot1x
Sysauthcontrol                    = Enabled
Dot1x Protocol Version            = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both

zrhlab-3550b#
```

**show dot1x all | interface XX** -- show status of interface

```
zrhlab-3550b#sh dot1x interface fastEthernet 0/20
PortStatus        = AUTHORIZED(GUEST-VLAN)
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 99

zrhlab-3550b#
```

**Troubleshooting hints**

Authentication is not working:
- is dot1x enabled on the interface?
- is dot1x enabled in global mode? check with show dot1x
- is it correct port type?
- multiple MAC address problem
- Is aaa enabled?

Example:
```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

**VLAN send by Radius ignored by Switch:**

- AAA server not correct configured -- check with "debug radius" VLAN is send by AAA server or in RDS.log of ACS. Also make sure, that each attribute must have a common tag value between 1 and 31 to identify the grouped relationship (in example below, Tag value is 1). IETF 81 (Tunnel Private Group ID):
- If AAA server sends those attributes, check if Switch accepts it by "debug dot1x all". If Switch is not accepting it, you will see something like:
  ```
  dot1x-ev:Received VLAN is No Vlan
  dot1x-ev:Received VLAN Id -1
  ```

- No authorization configured (IOS - Make sure you enable AAA and specify the authentication, and authorization methods.)

  Note: RADIUS attributes received in CatOS are automatically implemented if 802.1x is enabled. However, this is NOT the case for IOS. For IOS you need to configure the following command for the switch to accept config commands via RADIUS:

  ```plaintext
  Switch(config)# aaa new-model
  Switch(config)# aaa authentication dot1x default group radius
  Switch(config)# aaa authorization network default group radius
  ```

- VLAN is not existing on the switch -> Check with "show vlan brief" (Vlan should appear as active)

- Wrong VLAN attribute (Make sure the name of the VLAN matches what is configured in your ACS Server), check if Switch supports VLAN name or VLAN number!

- Switch is not supporting VLAN assignment at all --> This is true for SI images. Verify this with show version:

  ```
  Processor board ID FOC0725Y4DF
  Last reset from system-reset
  Running Standard Image
  24 FastEthernet/IEEE 802.3 interface(s)
  ```

  Note: If SI or EI is running on a 2950 Switch is hardware dependent! (Not image dependent)

**Taking Sniffer trace (client on Fa0/20 Sniffer on Fa0/13):**

```plaintext
monitor session 1 source interface Fa0/20
monitor session 1 destination interface Fa0/13
```

**Debugs:**

```plaintext
debug aaa authentication
debug radius
debug dot1x all
```

***
Enable 802.1x tracing on CatOS platforms

```plaintext
'set trace dot1x <level>'

"level" is a detail level value between 0-15
15 will do a full packet dump!
10 is usually good enough for most troubleshooting
Don't forget to disable tracing once you are done! 'set trace all 0'
```

***
Enable tracing and logging in the supplicant

```plaintext
'netsh ras set tr * enable'
Enables supplicant tracing and logging.
Creates logging debug files in "%systemRoot%/tracing"
Disable it with the command 'netsh ras set tr * disable'
```
16:30:35: ElMediaSenseCallbackWorker: Entered
16:30:35: ElMediaSenseCallbackWorker: For interface (Intel(R) 82559 Fast Ethernet LAN on Motherboard), GUID {0D7295D2-5F81-4A62-A494-AA3D4239CF49}, length of block = 94
16:30:35: ElMediaSenseCallbackWorker: Callback for sense connect
16:30:36: ElIoCompletionRoutine called, 60 bytes xferred
16:30:36: ElReadCompletionRoutine entered, 60 bytes recvd
16:30:36: ProcessReceivedPacket entered, length = 60
16:30:36: ProcessReceivedPacket: EAP_Packet
16:30:36: ProcessReceivedPacket: EAPOLSTATE_CONNECTING
16:30:36: TIMER: Restart PCB Time: 2097148
16:30:36: FSMAcquired entered for port Intel(R) 82559 Fast Ethernet LAN on Motherboard - Packet Scheduler Miniport
16:30:36: TIMER: Restart PCB Time: 30
16:30:36: FSMAcquired entered for port Intel(R) 82559 Fast Ethernet LAN on Motherboard - Packet Scheduler Miniport
16:30:36: TIMER: Restart PCB Time: 30
16:30:36: TIMER: Restart PCB Time: 30
16:30:36: TIMER: Restart PCB Time: 30
16:30:36: TIMER: Restart PCB Time: 30
16:30:36: ElWriteToInterface entered
16:30:36: ElWriteToPort: pPCB = 0009FE78, RefCnt = 4
16:30:36: ElWriteToInterface entered
16:30:36: ElWriteToPort: pPCB = 0009FE78, RefCnt = 3
16:30:36: ElWriteToPort entered: Pkt Length = 32
16:30:36: Identity sent out = ESELABS\Administrator
16:30:36: ElGetUserIdentity entered
16:30:36: ElGetEapUserInfo: Get value succeeded
16:30:36: ElGetEapUserInfo: Get value succeeded
16:30:36: ElGetUserIdentityOptimized: Get identity = ESELABS\Administrator
16:30:36: ElGetUserIdentity: ElGetUserIdentityOptimized got identity without user module intervention
16:30:36: ElGetUserIdentity completed with error 0
16:30:36: ElGetUserIdentity entered
16:30:36: ElGetEapUserInfo: Get value succeeded
16:30:36: ElGetUserIdentity: ElGetUserIdentityOptimized got identity without user module intervention
16:30:36: ElGetUserIdentity: ElGetUserIdentityOptimized got identity without user module intervention
Examining the RASTLS log

16:30:36:119: PeapReadConnectionData
16:30:36:119: PeapReadUserData
16:30:36:119: RasEapGetInfo
16:30:37:301: EapPeapBegin
16:30:37:311: PeapReadConnectionData
16:30:37:311: PeapReadUserData

EapTlsBegin(ESELABS\Administrator)
State change to Initial
EapTlsBegin: Detected 8021X authentication
EapTlsBegin: Detected PEAP authentication
MaxTLSMessageLength is now 16384
EapPeapBegin done
EapPeapMakeMessage
EapPeapCMakeMessage
PEAP:PEAP_STATE_INITIAL
EapTlsCMakeMessage
EapTlsReset
No Cert Store. Guest Access requested
No Cert Name. Guest access requested
Will validate server cert
MakeReplyMessage
SecurityContextFunction
InitializeSecurityContext returned 0x90312
State change to SentHello
BuildPacket
Sending Response (Code: 2) packet: Id: 2, Length: 80, Type: 13, TLS blob length: 70. Flags: L
EapPeapCMakeMessage done
EapPeapMakeMessage done

Radius Debug Decoded on Switch

Oct 24 15:24:40.165: AAA: parse name=FastEthernet0/20 idb type=-1 tty=-1
Oct 24 15:24:40.165: AAA: name=FastEthernet0/20 flags=0x15 type=7 shelf=0 slot=0 adapter=0 port=20 channel=0
Oct 24 15:24:40.165: AAA: parse name= idb type=-1 tty=-1
Oct 24 15:24:40.165: AAA/MEMORY: create_user (0x110A560) user='TOSTER\tom' ruser='TOSTER\tom' port='FastEthernet0/20' rem_addr=''
authen_type=EAP service=802.1x priv=1
Oct 24 15:24:40.165: AAA/AUTHEN/START (2878918934): port='FastEthernet0/20' list='Dot1x Acc List' action=LOGIN service=802.1x
Oct 24 15:24:40.165: RADIUS: ustruct sharecount=1
Oct 24 15:24:40.165: RADIUS: EAP-login: NAS Port = 00-08-a1-23-2f-7c RemAddr =0008.a123.2f7c
Oct 24 15:24:40.165: RADIUS: EAP-login: length of radius packet = 110 code = 1
Oct 24 15:24:40.165: RADIUS: Initial Transmit FastEthernet0/20 id 148 10.0.0.2:1812, Access-Request, len 110
Oct 24 15:24:40.165: NAS-IP-Address 10.0.0.199
Oct 24 15:24:40.165: NAS-Port-Type 0
Oct 24 15:24:40.165: User-Name "TOST"
Oct 24 15:24:40.165: Service-Type 2
Oct 24 15:24:40.165: Calling-Station-Id "00-0"
Oct 24 15:24:40.165: Confused about 79 17 0256000F
Oct 24 15:24:40.169: RADIUS: Received from id 148 10.0.0.2:1812, Access-Challenge, len 110
Oct 24 15:24:40.169: Confused about 79 255 014F03F4
Oct 24 15:24:40.169: Confused about 79 255 4953532D
Oct 24 15:24:40.169: RADIUS: EAP-login: NAS Port = 00-08-a1-23-2f-7c RemAddr =0008.a123.2f7c
Oct 24 15:24:40.169: RADIUS: EAP-login: length of radius packet = 208 code = 1
Oct 24 15:24:40.169: RADIUS: Initial Transmit FastEthernet0/20 id 149 10.0.0.2:1812, Access-Request, len 208
Oct 24 15:24:40.169: NAS-IP-Address 10.0.0.199
Oct 24 15:24:40.169: NAS-Port-Type 0
Oct 24 15:24:40.169: User-Name "TOST"
Oct 24 15:24:40.169: Service-Type 2
Oct 24 15:24:40.169: Calling-Station-Id "00-0"
Oct 24 15:24:40.169: Confused about 79 82 02480050
Oct 24 15:24:40.169: Confused about 80 18 04A7342A
Oct 24 15:24:40.169: RADIUS: Received from id 149 10.0.0.2:1812, Access-Challenge, len 1091
Oct 24 15:24:40.169: Confused about 79 255 01FD93F4
Oct 24 15:24:40.169: Confused about 79 255 4953532D
Oct 24 15:24:42.869: RADIUS: ustruct sharecount=1
Oct 24 15:24:42.869: RADIUS: EAP-login: NAS Port = 00-08-a1-23-2f-7c RemAddr =0008.a123.2f7c
Oct 24 15:24:42.869: RADIUS: EAP-login: length of radius packet = 134 code = 1
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 153 10.0.0.2:1812, Access-Request, len 134
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 79 8 02520006
Oct 24 15:24:42.869: Confused about 80 18 6884BA26
Oct 24 15:24:42.869: RADIUS: Received from id 153 10.0.0.2:1812, Access-Challenge, len 101
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 6705B93
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 154 10.0.0.2:1812, Access-Request, len 166
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 16FC2C92
Oct 24 15:24:42.869: RADIUS: Received from id 154 10.0.0.2:1812, Access-Challenge, len 128
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 5485BD78
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 155 10.0.0.2:1812, Access-Request, len 220
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 428B6BBD
Oct 24 15:24:42.869: RADIUS: Received from id 155 10.0.0.2:1812, Access-Challenge, len 128
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 14535C78
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 156 10.0.0.2:1812, Access-Request, len 220
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 9BFD2A3A
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 157 10.0.0.2:1812, Access-Request, len 220
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 5485BD78
Oct 24 15:24:42.869: RADIUS: Initial Transmit FastEthernet0/20 id 158 10.0.0.2:1812, Access-Request, len 220
Oct 24 15:24:42.869: NAS-IP-Address 10.0.0.199
Oct 24 15:24:42.869: NAS-Port-Type 0
Oct 24 15:24:42.869: User-Name "TOST"
Oct 24 15:24:42.869: Service-Type 2
Oct 24 15:24:42.869: Framed-MTU 5
Oct 24 15:24:42.869: Calling-Station-Id "00-0"
Oct 24 15:24:42.869: State "CISC"
Oct 24 15:24:42.869: Confused about 80 18 9BFD2A3A

http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html
IEEE

http://www.ieee.com/portal/index.jsp

<table>
<thead>
<tr>
<th>IEEE Terms</th>
<th>Normal People Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant</td>
<td>Client</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Network Access Device</td>
</tr>
<tr>
<td>Authentication Server</td>
<td>AAA/RADIUS Server</td>
</tr>
</tbody>
</table>

Lab Config

Note: For CatOS see FAQ below

zrhlab-3550b#sh run
Building configuration...

Current configuration : 4523 bytes
!
! Last configuration change at 11:18:47 UTC Fri Oct 17 2003 by cisco
! NVRAM config last updated at 11:18:48 UTC Fri Oct 17 2003 by cisco
!
version 12.1
no service pad
service timestamps debug datetime msec
service timestamps log uptime
no service password-encryption
!
hostname zrhlab-3550b
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
enable password cisco
!
username cisco password 0 cisco
ip subnet-zero
ip routing
!
ip dhcp pool guest
  network 10.0.99.0 255.255.255.0
  default-router 10.0.99.254
  domain-name cisco.com
!
ip dhcp pool Zurich
  network 10.0.120.0 255.255.255.0
  default-router 10.0.120.254
  domain-name cisco.com
!
ip dhcp pool Gland
  network 10.0.110.0 255.255.255.0
  default-router 10.0.110.254
  domain-name cisco.com
!
ip dhcp pool Machine
  network 10.0.100.0 255.255.255.0
  default-router 10.0.100.254
  domain-name cisco.com
!

http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html

10.11.2003
no ip domain-lookup
ip domain-name toster.com
ip name-server 10.51.80.190
ip name-server 10.0.0.2
vtp mode transparent
!
spanning-tree mode pvst
spanning-tree extend system-id
dot1x system-auth-control
!
vlan 2
  name ACS
!
vlan 10
  name Cisco
!
vlan 99
  name Guest
!
vlan 100
  name Machine
!
vlan 110
  name Gland
!
vlan 120
  name Zurich
!
interface FastEthernet0/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 10
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/4
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/5
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/6
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/7
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/8
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/9
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/10
  switchport access vlan 10
  switchport mode access
  spanning-tree portfast
!
interface FastEthernet0/11
interface FastEthernet0/12
   switchport access vlan 10
   switchport mode access
   spanning-tree portfast
!
interface FastEthernet0/13
   switchport mode dynamic desirable
!
interface FastEthernet0/14
   switchport mode dynamic desirable
!
interface FastEthernet0/15
   switchport mode dynamic desirable
!
interface FastEthernet0/16
   switchport mode dynamic desirable
!
interface FastEthernet0/17
   switchport mode dynamic desirable
!
interface FastEthernet0/18
   switchport mode dynamic desirable
!
interface FastEthernet0/19
   switchport mode dynamic desirable
!
interface FastEthernet0/20
   switchport node access
dot1x port-control auto
dot1x guest-vlan 99
   spanning-tree portfast
!
interface FastEthernet0/21
   switchport node access
dot1x port-control auto
dot1x guest-vlan 99
   spanning-tree portfast
!
interface FastEthernet0/22
   switchport node access
dot1x port-control auto
dot1x guest-vlan 99
   spanning-tree portfast
!
interface FastEthernet0/23
   switchport trunk encapsulation dot1q
   switchport trunk allowed vlan 1,99,100,110,120
   switchport mode trunk
!
interface FastEthernet0/24
   switchport access vlan 2
   switchport mode access
!
interface GigabitEthernet0/1
   switchport mode dynamic desirable
!
interface GigabitEthernet0/2
   switchport mode dynamic desirable
!
interface Vlan1
   no ip address
   shutdown
!
interface Vlan2
   ip address 10.51.80.150 255.255.255.0
!
interface Vlan10
   ip address 10.0.0.199 255.255.255.0
!
interface Vlan99
   ip address 10.0.99.254 255.255.255.0
!
interface Vlan100
   ip address 10.0.100.254 255.255.255.0
!
interface Vlan110
   ip address 10.0.110.254 255.255.255.0
!
interface Vlan120
   ip address 10.0.120.254 255.255.255.0
!
ip default-gateway 10.51.80.254
ip classless
ip route 0.0.0.0 0.0.0.0 10.51.80.254
ip http server
!
!
radius-server host 10.0.0.2 auth-port 1812 acct-port 1813 key cisco
radius-server retransmit 3
!
line con 0
line vty 0 4
exec-timeout 0 0
password cisco
line vty 5 15
!
ntp clock-period 17180217
ntp server 144.254.49.187
!
monitor session 1 source interface Fa0/20
monitor session 1 destination interface Fa0/13
end

zrhlab-3550b#

FAQ

Q1: Does the Catalyst XXX support EAP-XXX?
A1: The switches are transparent to the EAP method used. The switch typically does not need to “support” an EAP method.

Q2: Will the Catalyst XXXXX XL platform get 802.1x?
A2: No. There will be no upgrades or enhancements to the Catalyst XL switches to add 802.1x or any identity features. This is primarily because of a hardware limitation problem. There isn’t enough code space to include 802.1x features and fix any potential bugs later on.

Q3: How does our 802.1x strategy fit with our VoIP solutions?
A3: Two phases of VoIP and 802.1x support.
- 802.1x with VVID – Unauthenticated Voice VLAN (VVID) access, Authenticated Data VLAN (PVID) access. This leaves voice no better than it is today, but allows 802.1x and VoIP to co-exist at the same time.

Q4: How to connect a PC (dot1x client) through an IP Phone (non-dot1x client) to a dot1x enabled switch port?
A4: Switch identifies IP Phone (as a Cisco phone) and bypasses dot1x authentication – BUT – still forces authentication for downstream device

802dot1XonSwitches
802.11.2003
http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html
**Q5: Operating System 802.1x Support?**

**A5:** Windows see above.

- Linux - Open Source or 3rd Party (MeetingHouse) http://www.open1x.org
- Solaris – Open Source or 3rd Party via MeetingHouse Communications http://www.mtghouse.com
- Apple Supplicant: Apple has an integrated working 802.1x supplicant in Panther (OS X 10.3) – no current ETA on FCS (possibly late Q4CY2003).
  ESE is currently testing and troubleshooting for Apple. (Yes, we have Macs ?)
  Currently supported EAP methods are pretty much everything!
  - EAP-TLS
  - LEAP
  - EAP-TTLS
  - PEAP with any sub-type
  - EAP-GTC
  - MS-CHAPv2

**Q6: Which Cisco Platforms Support IBNS?**

**A6:** (Features will be limited by platform capabilities.)

- Catalyst 5500 – Basic 802.1x only
- Catalyst 6000/4000 - IBNS
- Catalyst 2950/3550 – IBNS
- Aironet WLAN APs – Some IBNS
- Cisco 800 series – IBNS Subset

**Q7: Feature details?**

**A7:**

- Centralized Management with AAA server
- Wireless Mobility with 802.1X and EAP Authentication Types
- Catalyst Switch Portfolio
- Basic 802.1X Support
- 802.1X with VLANs
- 802.1X with Port Security
- 802.1X with VVID
- 802.1X Guest VLANs
- 802.1X with ACLs

---

**Catalyst 6500**

- CatOS
  - 7.5.1
  - 802.1x w/ VLAN Assignment
  - 802.1x w/ VVID
  - 802.1x w/ Guest VLAN
  - 802.1x w/ Port Security
  - 7.6.1
  - 802.1x w/ DHCP

---

http://www-tac.cisco.com/~fariesen/802.1x/802dot1XonSwitches_customer_version.html  
10.11.2003
12.1(13)E
802.1x w/ VLAN Assignment

Catalyst 4000/4500
CatOS
7.5.1
802.1x w/ VLAN Assignment

IOS
12.1(19)EW – June ’03
802.1x w/ VLAN Assignment
802.1x Guest VLAN

Catalyst 3550/2950/3750
2950/2955
12.1(12c)EA1
802.1x w/ VLAN Assignment
802.1x w/VVID
802.1x w/ Port Sec
12.1(14)EA1
802.1x Guest VLAN

3550 (EMI/SMI)
12.1(12c)EA1
802.1x w/ VLAN Assignment
802.1x w/VVID
802.1x w/ Port Sec
12.1(14)EA1
802.1x Guest VLAN

3750
802.1x w/ VLAN Assignment
802.1x w/VVID
802.1x Guest VLAN
802.1x w/ DHCP
802.1x w/ ACL/QoS

Cisco ACS Server

3.2 Avail Now
Appliance
Microsoft Peap
PEAP Proxy
Machine Auth
EAP Type Negotiation
LDAP Multithreading
EAP Performance
Windows password

Q9: CatOS Config?
A9:
# RADIUS configuration
set radius server <ip_address> auth-port 1812 primary
set radius key <key>

# Global 802.1x configuration
set dot1x system-auth-control enable
set dot1x quiet-period 10 (default: 30)
set dot1x tx-period 10 (default: 30)
set dot1x supp-timeout 5 (default: 30)
set dot1x server-timeout 5 (default: 30)
set dot1x max-req 4 (default: 2)
set dot1x re-authperiod

# Port Level 802.1x configuration
set port dot1x <mod/port> port-control auto
set port dot1x <mod/port> port-control force-authorized
set port dot1x <mod/port> multiple-host enable/disable
set port dot1x <mod/port> re-authentication enable/disable

MS Case SRQ031001601501 summary

[ARCR]
ACTION:

authenticate a 802.1x wired connection on windows 2000 SP4 and Windows XP SP1

RESULT:

the authentication did not work, and if it worked DHCP IP address assignment did not work as expected

The same config did work with wireless connections

CAUSE:

-for wired connections the default settings for 802.1x connection differs from that for wireless connections

-there was a bug in the DHCP client implementation

RESOLUTION:

-to solve the problem you have to

A) change the following reg.-keys:

Software\Microsoft\EAPOL\Parameters\General\Global

SupplicantMode

REG_DWORD

0: Disable IEEE 802.1X operation.
1: Inhibit transmission of EAPOL-Start and EAPOL-Logoff packets under all scenarios.
2: Include learning to determine when to initiate the transmission of EAPOL packets.
3: Compliant with IEEE 802.1X Specification.

Key needs to be set to 3 for your environment

Software\Microsoft\EAPOL\Parameters\General\Global

AuthMode

REG_DWORD

0: Machine authentication mode in Windows XP Client RTM. When a user logs in, if the connection has already been authenticated with Machine credentials, the user’s credentials are not used for authentication.
1: Machine authentication with re-authentication functionality. Whenever a user logs in, 802.1X authentication is performed using the user’s credentials.
2: Machine authentication only - Whenever a user logs in, it has no effect on the connection. 802.1X authentication is performed using machine credentials only.

This key has to be set to 1.

B) for Windows 2000 you have to install Hotfix 823859 "EapType 26 Failed in RasEapMakeMessage and Returned 0x80004005" Error, the related KB article is 816757 "EapType 26 Failed in RasEapMakeMessage and Returned 0x80004005" Error

http://support.microsoft.com/?id=816757

the hotfix is included in SP5

and hotfix

822596 DHCP Does Not Obtain a New Address When EAP Reauthenticates Across

<http://support.microsoft.com/?id=822596>
(although the description tells that this is a Windows XP hotfix only the fix is also available for Windows 2000)

(also included with SP5)

to make DHCP also working correctly in Windows XP you have to install hotfix

826239 Small Delay in Logon to Network When You Use a Wireless Network

http://support.microsoft.com/?id=826239