

Network Access Security – It's Broke, Now What?

June 15, 2010

Jeffrey L Carrell

Network Security Consultant | Network Conversions

SHARKFEST '10

Stanford University

June 14-17, 2010

SHARKFEST '10

Network Access Security – It's Broke, Now What?

- Access Problems on the Network
- How to Solve It
- How to Enhance It
- Now it Works
- Now it's Broken

Network Access Security – It's Broke, Now What?

- The Issue: Open Access LAN Switch Ports
- Authentication of Users and End-point Devices on a LAN
- Enhanced Policy Decisions after Initial Authentication
- Network Access Control/Protection
- Components of a Secure Access System
- Demonstration of an 802.1X System

The Issue: Open Access LAN Switch Ports

- Are there open or available LAN Switch ports?
- Can the client device get an IP address?
- Can the client gain “any” access to network?
- If so, then there is the possibility of network attacks
 - attacks to network infrastructure devices (switches, APs)
 - attacks to network resources (servers, etc)
 - attacks to end-user computers
 - virus, trojan, and other malware distribution
 - use of network for malicious network attacks - inside and/or outside
 - data privacy exploits

Controlling Access to the Network

- Lock down LAN switch ports with configuration that requires all connections to the switch to authenticate
 - Users Authenticate
 - providing userid/password credentials
 - can be automated for single sign-on
 - Devices Authenticate
 - VoIP phones
 - Printers
 - Surveillance Cameras

Authentication of Users and End-point Devices on a LAN

- Authentication System for End-point Devices on a Local Area Network
 - IEEE 802.1X
- The Challenge - Adding VoIP Phones to the Secure Network
- RFC-4675
 - Enhancements to IEEE 802.1X

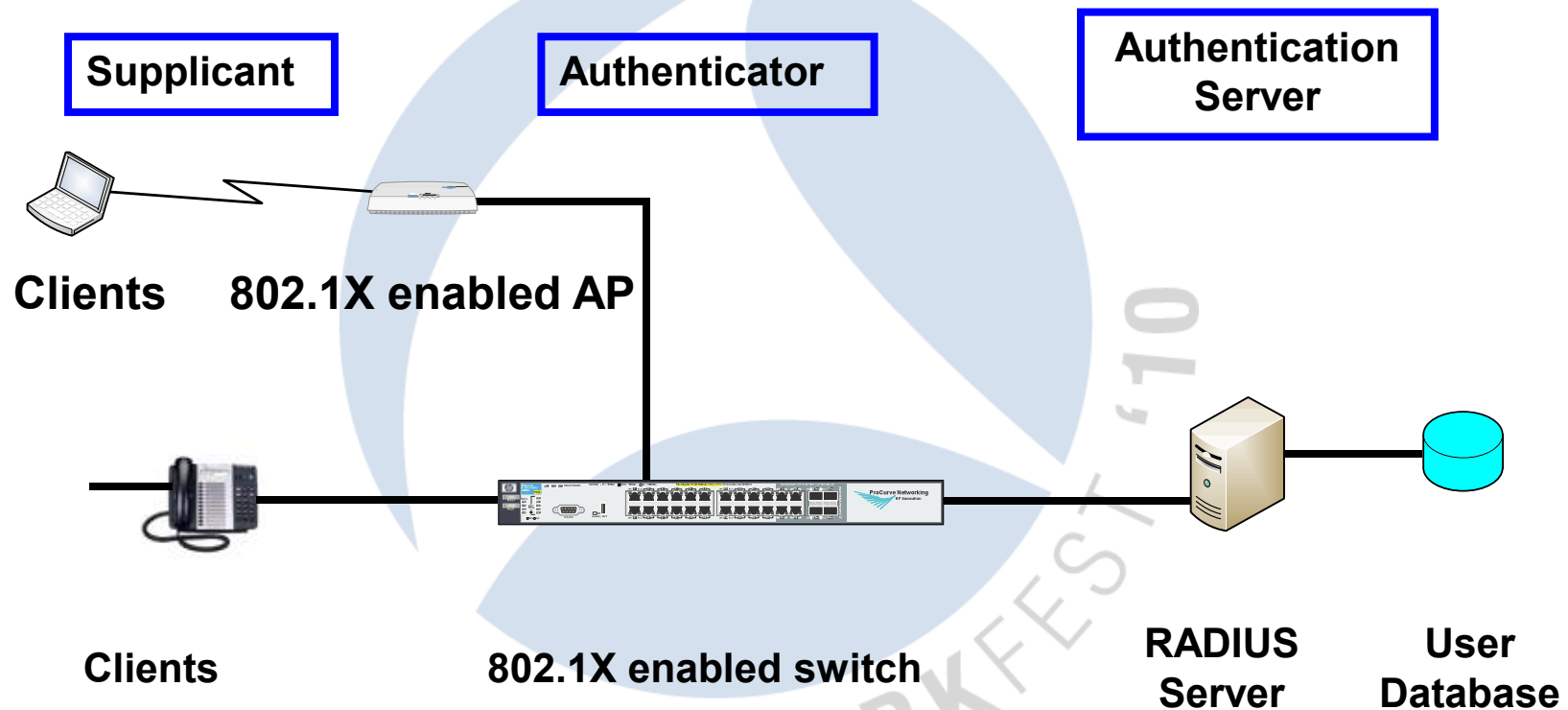
What is IEEE 802.1X?

- IEEE 802.1X is a standards based mechanism allowing users and end-point devices to authenticate in order to gain network access
- Foundation relies on the Remote Authentication Dial-In User Service (RADIUS) networking protocol for Authentication, Authorization and Accounting (AAA) management
- Devices communicate via the Extensible Authentication Protocol over LAN (EAP-OL) - a Layer 2 communication to the authenticator

Why IEEE 802.1X?

- 802.1X controlled switch ports block “normal” traffic by default until authentication is verified using a RADIUS server and EAP
- For specific user authentication, RADIUS server can provide VLAN ID (VID) to switch
- 802.1X does not specify what EAP type is used, as long as the supplicant and authentication server agree on an EAP method
- 802.1X is an IEEE standard and therefore provides interoperability between standards-based network access equipment, authentication servers, and client supplicants

Components of an 802.1X System



Authentication Server

- Microsoft IAS (Windows Server 2000/2003)
- Microsoft NPS (Windows Server 2008)
- Juniper Networks Steel-Belted Radius (multiple server platforms)
- FreeRADIUS (many linux server platforms)
- Other RADIUS – conforming to RFC's
 - RFC 2284 PPP Extensible Authentication Protocol (EAP)
 - RFC 2865 Remote Authentication Dial In User Service (RADIUS)
 - RFC 2869 RADIUS Extensions

Authenticator

- 802.1X Enabled LAN Switch
- 802.1X Enabled Wireless Access Point
- (generally requires enterprise-class devices)

Supplicant

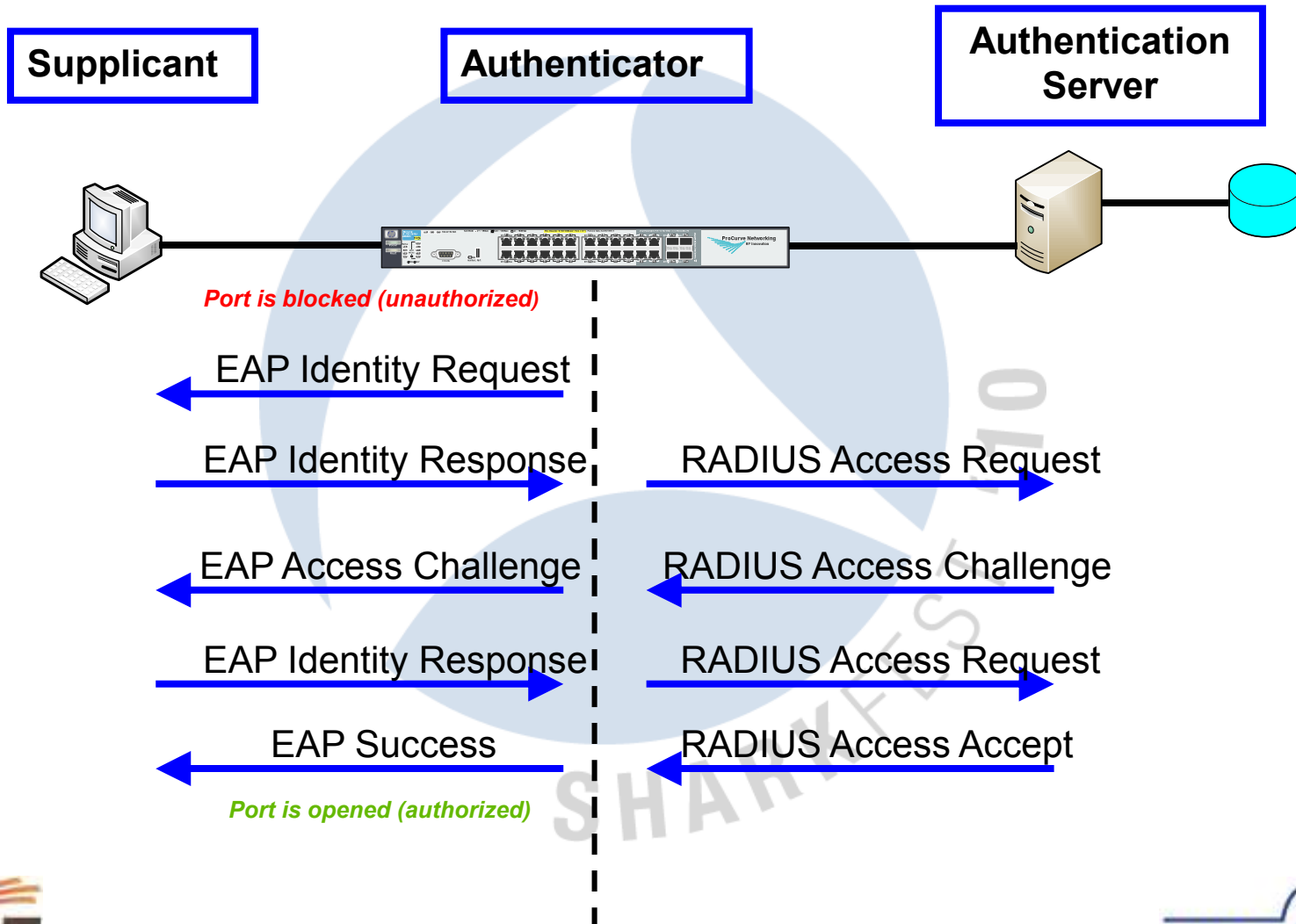
- Microsoft – WinXP, Vista, Win7
- Apple – Mac OS X 10.4+
- Juniper Networks – Odyssey Access Client (Windows, Red Hat Linux)
- Open Source - Open1X (Windows, Linux)
- Network Printers (built-in)
- VoIP Phones (built-in)
- LAN Switch (built-in)
- Wireless Access Point (built-in)

- Client **MUST** be configured for the same EAP type supported on the Authentication Server

EAP types

- EAP-MD5
 - least secure
 - most commonly supported on VoIP phones
- Protected EAP (EAP-PEAP)
 - more secure, can use digital certificate on end-point
- EAP-Tunneled TLS (EAP-TTLS)
 - more secure, can use digital certificate on end-point
- EAP-Transport Layer Security (EAP-TLS)
 - most secure, requires digital certificate on end-point

802.1X Communications Flow



Switch Port States in 802.1X

- A port that has been configured to require 802.1X authentication has two states:
 - **Unauthorized**—no authorized client has connected to the port, or client has failed authentication
 - **Authorized**—connected client has supplied valid credentials and has been authenticated
- When a port is in the **unauthorized** state, only EAP traffic is allowed
- When a port is in the **authorized** state, traffic is forwarded normally

VLAN Assignment of Switch Port

- RADIUS can send attributes to the switch which could define a specific VLAN the port is assigned to based on the user credentials
- If RADIUS doesn't provide VLAN attributes, switch port could be assigned to "authorized VID"
- If RADIUS doesn't provide VLAN attributes and the "authorized VID" is not defined, then the switch opens the port using the statically assigned VID of that port

The Challenge - Adding VoIP Phones to the Secure Network

- Some manufacturers' VoIP phones support 802.1X with a built-in supplicant, but generally only a few in their product lines
 - if so, then a matching RADIUS remote access policy can be configured to support the VoIP phone
- Without RFC-4675, dynamic 802.1Q (tag) VID assignment from RADIUS is not possible
- If the VoIP phone doesn't have a supplicant, difficult to support 802.1X authentication
 - some LAN switch manufacturers support alternate 802.1X authentication methods, such as MAC Auth & WEB Auth

RFC-4675

Enhancements to 802.1X

- RADIUS can specify tag ports (for VoIP phones)
- RADIUS can specify VLAN name to switch
- Is supported on:
 - FreeRADIUS v2.0.0+
- May require LAN switch software upgrade

Configuring a Microsoft Server Based System for 802.1X

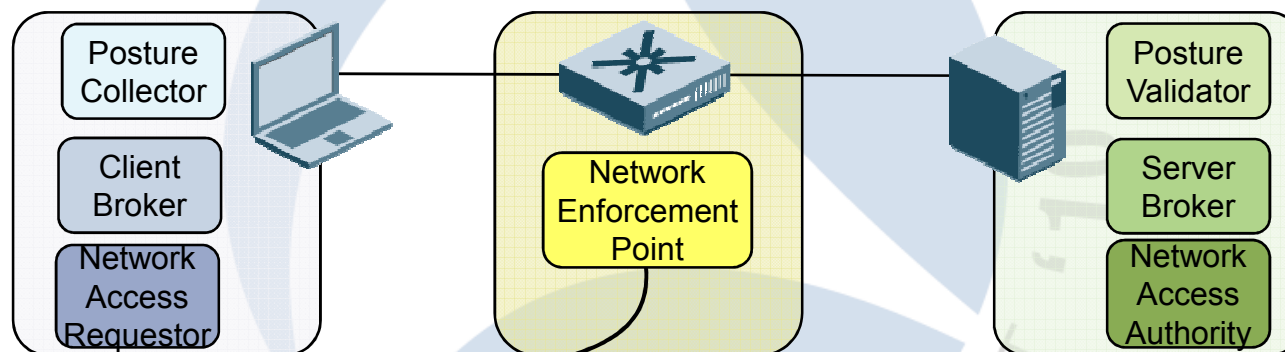
- Active Directory
 - userID(s) must have “remote access permission” enabled
- IAS/NPS
 - define each authenticator as RADIUS client
 - define remote access policies for users
- LAN Switch and/or AP
 - configure RADIUS server definition
 - configure specific ports/WLANs to support 802.1X
- Client Supplicant
 - configure EAP type used for authentication

Enhanced Policy Decisions after Initial Authentication

- A mechanism to apply additional policy based rules to validate a user's level of access into the network
- Executes after initial 802.1X authentication
- Policy components may include:
 - where is the user/device in the network
 - when is the user/device on the network
 - integrity of the computer or device

TCG/Microsoft/IETF Architectures

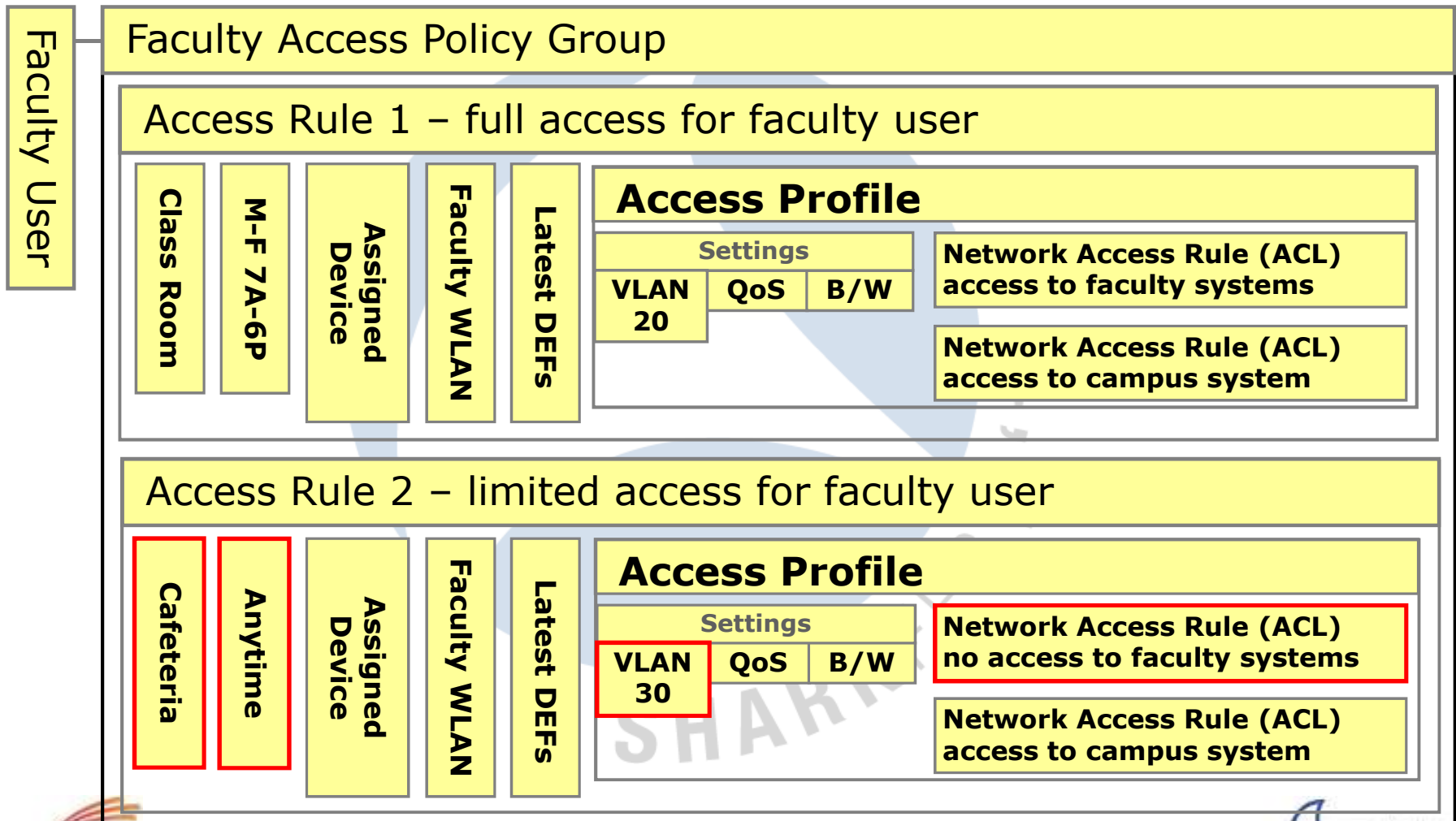
What is it?	TCG TNC	Microsoft	IETF NEA
Posture Collector Third-party software that runs on the client and collects information on security status and applications, such as "is A/V enabled and up-to-date?"	Integrity Measurement Collector	System Health Agent	Posture Collector
Client Broker "Middleware" that runs on the client and talks to the Posture Collectors, collecting their data, and passing it down to Network Access Requestor. In product form, this is generally bundled with the Network Access Requestor.	TNC Client	NAP Agent	Posture Broker Client
Network Access Requestor Software that connects the client to network. Examples might be 802.1X supplicant or IPSec VPN client. Used to authenticate the user, but also as a conduit for Posture Collector data to make it to the other side.	Network Access Requestor	NAP Enforcement Client	Posture Transport Client



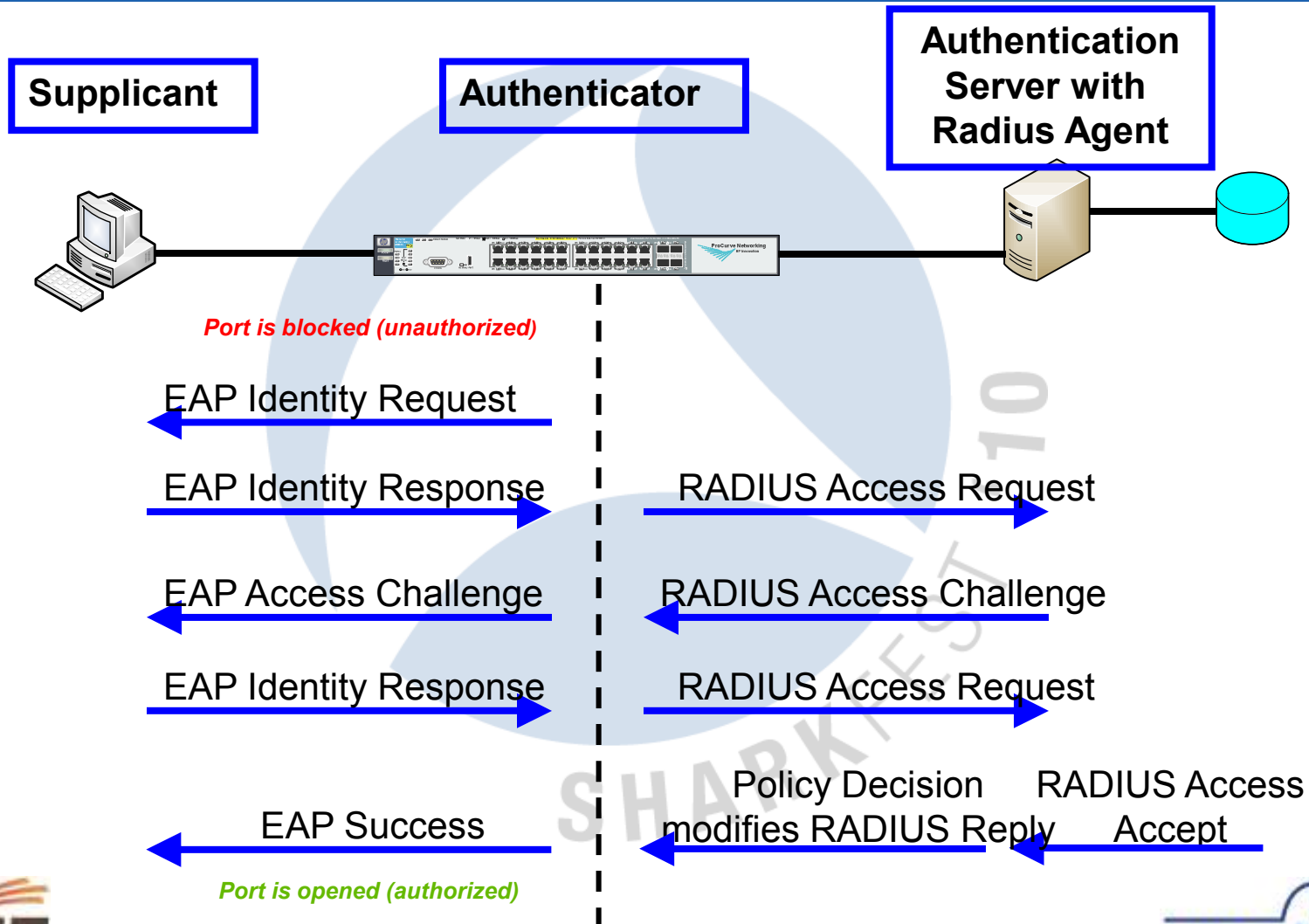
What is it?	TCG TNC	Microsoft	IETF NEA
Network Enforcement Point Component within the network that enforces policy, typically an 802.1X-capable switch or WLAN, VPN gateway, or firewall.	Policy Enforcement Point	NAP Enforcement Server	Intermediary Devices
Posture Validator Third-party software that receives status information from Posture Collectors on clients and validates the status information against stated network policy, returning a status to the Server Broker.	Integrity Measurement Verifier	System Health Validator	Posture Validator
Server Broker "Middleware" acting as an interface between multiple Posture Validators and the Network Access Authority.	TNC Server	NAP Administration Server	Posture Broker Server
Network Access Authority A server responsible for validating authentication and posture information and passing policy information back to the Network Enforcement Point.	Network Access Authority	Network Policy Server	Posture Transport Server

Enhanced Policy Decisions

Example Policy



Enhanced Policy Decisions Communications Flow



Network Access Control/Protection

- Before authentication and possible policy decision *
- Provides Endpoint Integrity Assessment
 - Verify OS updates & hot fixes/service packs
 - Verify security applications are running and up-to-date
- Provides Endpoint Integrity Enforcement
 - Quarantines access for remediation to NAC/NAP policy compliance
 - Restrict access for non-compliance

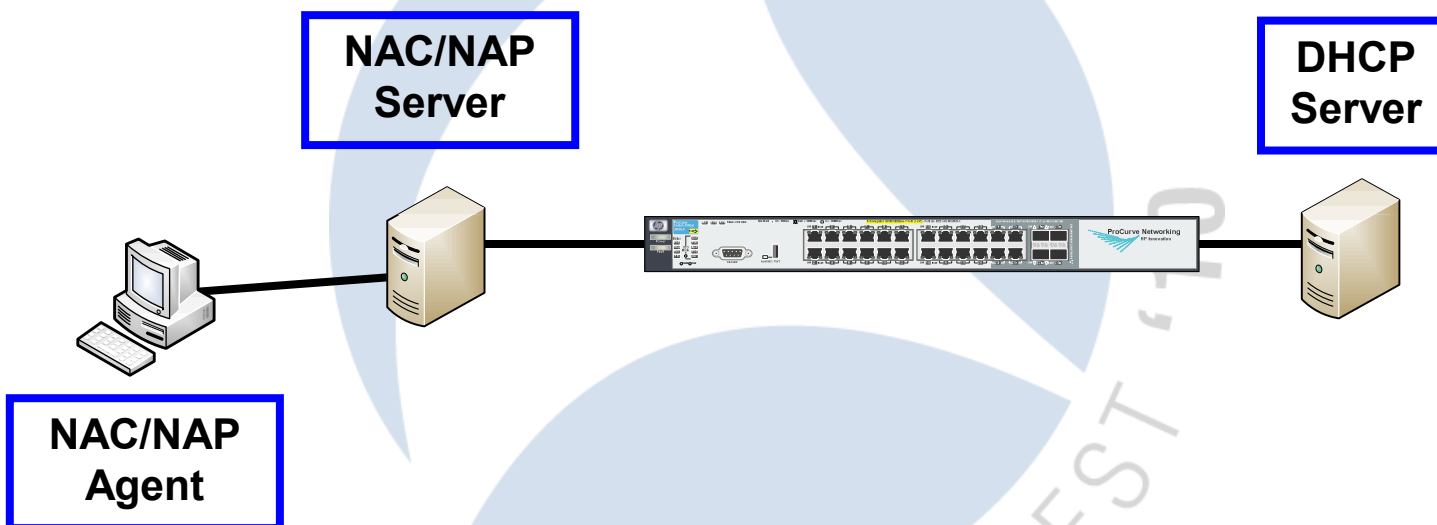
* Some NAC/NAP Systems include these functions

Network Access Control/Protection

- 3 Primary client testing options
 - Agent – least user interaction
 - ActiveX – requires user to launch browser
 - Agentless – limited function
- 3 Types of Endpoint Integrity Assessment Tests
 - Inline – NAC/NAP server in the flow of traffic
 - DHCP – NAC/NAP server intercepts DHCP request
 - 802.1X – authentication required

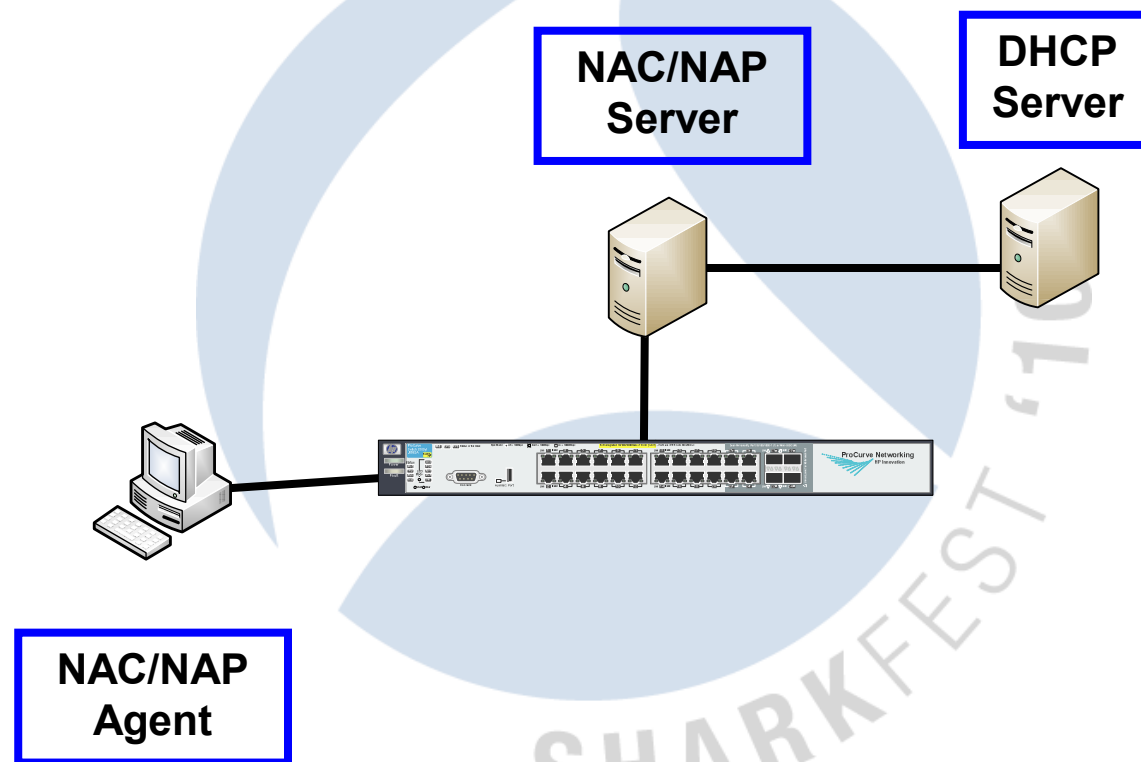
Endpoint Integrity Assessment Test – Inline

- NAC/NAP server in the flow of traffic



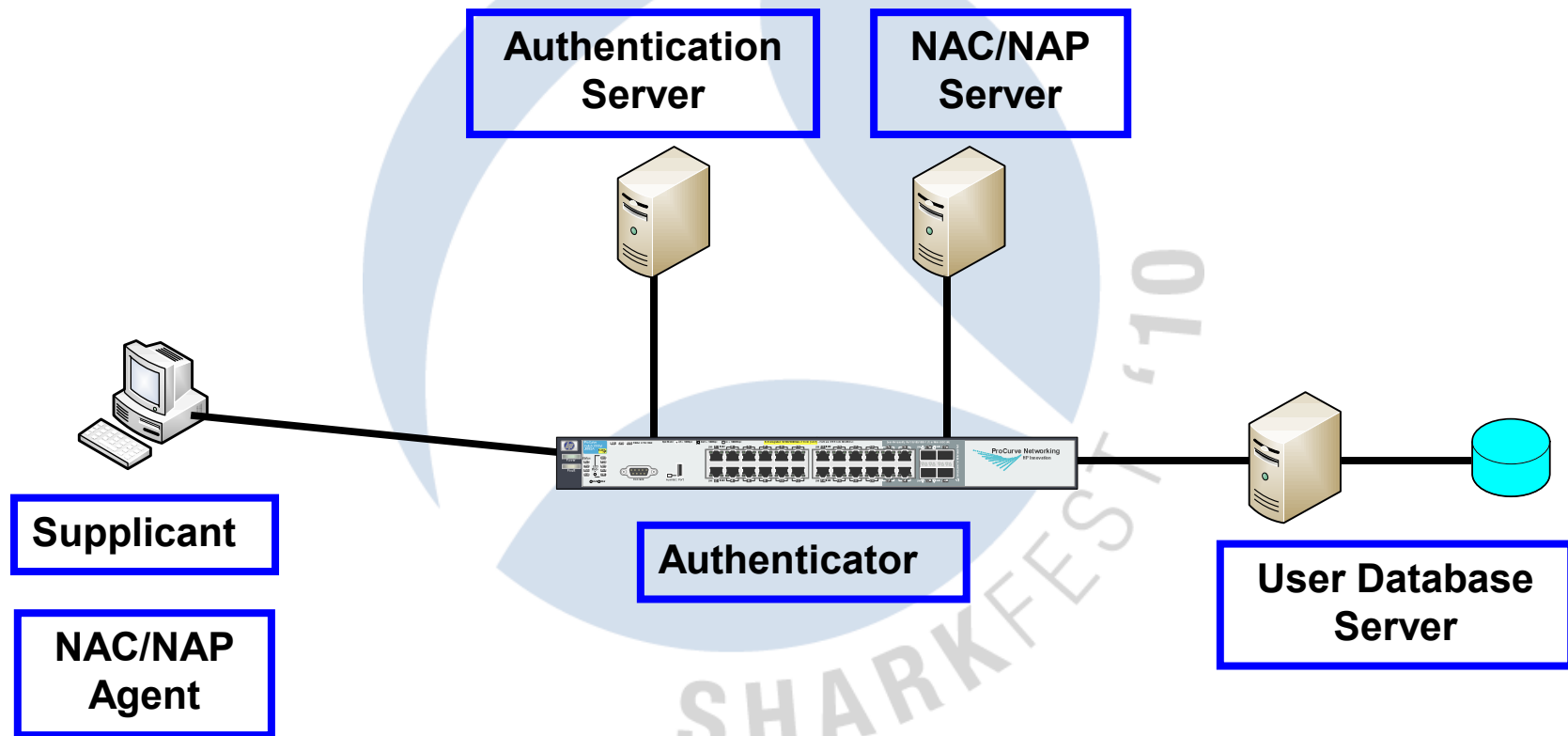
Endpoint Integrity Assessment Test – DHCP

- NAC/NAP server intercepts DHCP request

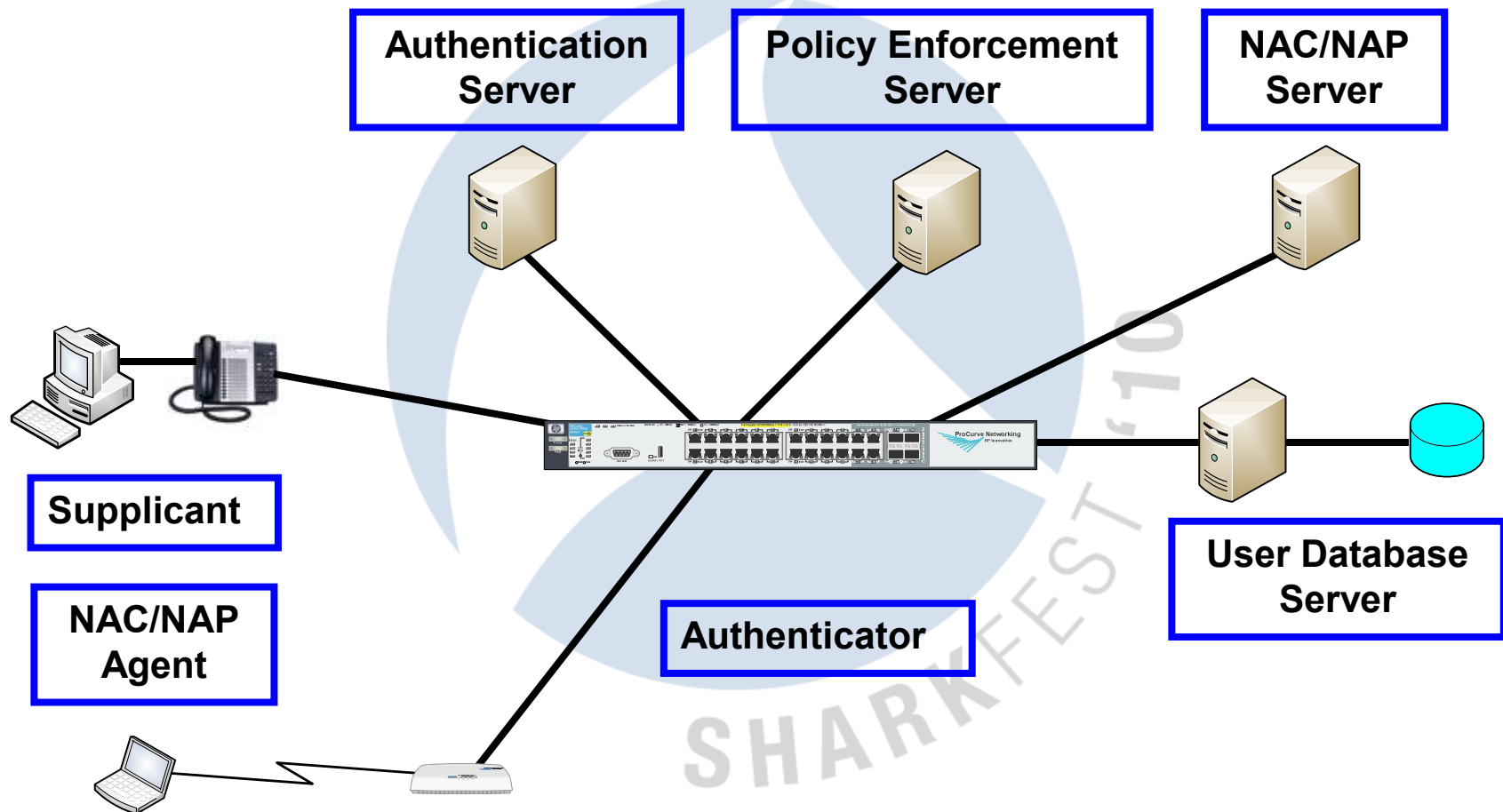


Endpoint Integrity Assessment Test – 802.1X

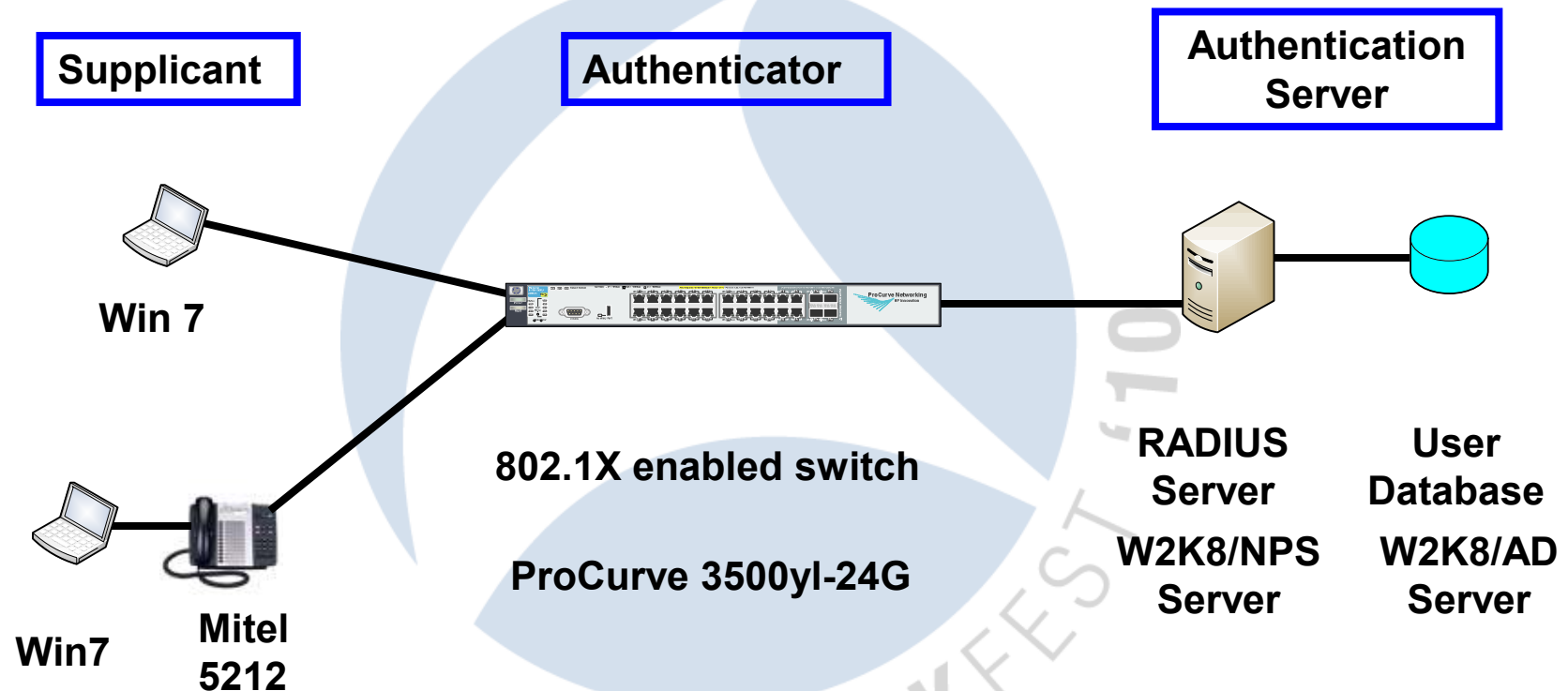
- Authentication required



Components of a Secure Access System



Demonstration of an 802.1X System



Of Course We Have Captures!

- Successful client authentication

Switch	winXP	EAP	Request, Identity [RFC3748]
winXP	Nearest	EAP	Response, Identity [RFC3748]
Switch	Radius_Server	RADIUS	Access-Request(1) (id=8, l=334)
Radius_Server	Switch	RADIUS	Access-challenge(11) (id=8, l=114)
Switch	winXP	EAP	Request, MD5-Challenge [RFC3748]
winXP	Nearest	EAP	Response, MD5-Challenge [RFC3748]
Switch	Radius_Server	RADIUS	Access-Request(1) (id=9, l=389)
Radius_Server	Switch	RADIUS	Access-Accept(2) (id=9, l=119)
Switch	winXP	EAP	Success

- Failed client authentication

Switch	win7	EAP	Request, Identity [RFC3748]
win7	Nearest	EAP	Response, Identity [RFC3748]
Switch	Radius_Server	RADIUS	Access-Request(1) (id=137, l=334)
Radius_Server	Switch	RADIUS	Access-challenge(11) (id=137, l=114)
Switch	win7	EAP	Request, MD5-Challenge [RFC3748]
win7	Nearest	EAP	Response, Legacy Nak (Response only) [RFC3748]
Switch	Radius_Server	RADIUS	Access-Request(1) (id=138, l=365)
Radius_Server	Switch	RADIUS	Access-Reject(3) (id=138, l=56)
Switch	win7	EAP	Failure

Successful Client Authentication, w/VLAN Assignment

```
592 2010-06-04 02:17:51.475649 Radius_Server Switch
+ Ethernet II, Src: Radius_Server (00:0C:29:04:15:55), Dst: Switch (00:1
+ Internet Protocol, Src: Radius_Server (10.0.100.111), Dst: Switch (10.
+ User Datagram Protocol, Src Port: radius (1812), Dst Port: radius (181
- Radius Protocol
  Code: Access-Accept (2)
  Packet identifier: 0x9 (9)
  Length: 119
  Authenticator: 9CF40A55A5FBD916B4A51D6AFDAEA774
  \[This is a response to a request in frame 581\]
  [Time from request: 1.997238000 seconds]
- Attribute Value Pairs
  + AVP: l=6 t=Framed-Protocol(7): PPP(1)
  + AVP: l=6 t=Service-Type(6): Framed-User(2)
  + AVP: l=6 t=Tunnel-Medium-Type(65): IEEE-802(6)
  + AVP: l=5 t=Tunnel-Private-Group-Id(81): 220
  + AVP: l=6 t=Tunnel-Type(64): VLAN(13)
```


Successful Client Authentication, but Fail on Switch

- RADIUS provided VID, switch did not have that specific VID configured

```
⊕ Frame 91 (161 bytes on wire, 161 bytes captured)
⊕ Ethernet II, Src: Radius_Server (00:0c:29:d4:15:55), Dst: Switch (00:16:35:b3:76:c0)
⊕ Internet Protocol, Src: Radius_Server (10.0.100.111), Dst: Switch (10.0.100.24)
⊕ User Datagram Protocol, Src Port: radius (1812), Dst Port: radius (1812)
⊖ Radius Protocol
  Code: Access-Accept (2)
  Packet identifier: 0xde (222)
  Length: 119
  Authenticator: E2852D76F355CCBB36BC258018327DFF
  \[This is a response to a request in frame 72\]
  [Time from request: 1.997872000 seconds]
⊕ Attribute Value Pairs
  ⊕ AVP: l=6 t=Framed-Protocol(7): PPP(1)
  ⊕ AVP: l=6 t=Service-Type(6): Framed-User(2)
  ⊕ AVP: l=6 t=Tunnel-Medium-Type(65): IEEE-802(6)
  ⊕ AVP: l=5 t=Tunnel-Private-Group-Id(81): 221
  ⊕ AVP: l=6 t=Tunnel-Type(64): VLAN(13)
```

Fri Jun 04 13:44:29 2010: <12> Jun 4 13:44:28 10.0.100.24 02400 dca: 8021X client, RADIUS-
assigned VID validation error. MAC 00226481699E port 17 VLAN-Id 0 or unknown.

Unsuccessful Authentication: no Supplicant Enabled on Client

Switch	win7	EAP	Request, Identity [RFC3748]
Switch	win7	EAP	Failure

- [-] Frame 428 (60 bytes on wire, 60 bytes captured)
 - Arrival Time: Jun 4, 2010 03:59:08.822225000
 - [Time delta from previous captured frame: 0.412181000 seconds]
 - [Time delta from previous displayed frame: 29.999518000 seconds]
 - [Time since reference or first frame: 95.534617000 seconds]
 - Frame Number: 428
 - Frame Length: 60 bytes
 - Capture Length: 60 bytes
 - [Frame is marked: False]
 - [Protocols in frame: eth:eapol:eap]
- [-] Ethernet II, Src: Switch (00:16:35:b3:76:c0), Dst: win7 (00:23:7d:e7:3a:db)
 - [-] Destination: win7 (00:23:7d:e7:3a:db)
 - [-] Source: Switch (00:16:35:b3:76:c0)
 - Type: 802.1X Authentication (0x888e)
 - Trailer: 00...
- [-] 802.1X Authentication
 - Version: 1
 - Type: EAP Packet (0)
 - Length: 15
- [-] Extensible Authentication Protocol
 - Code: Request (1)
 - Id: 2
 - Length: 15
 - Type: Identity [RFC3748] (1)
 - Identity (10 bytes): User name:



Fail-Client Configured for Incorrect EAP Type

Network Policy and Access Services 2,420 Events

2,420 Events

Level	Date and Time	Source	Event ID	Task C...
Information	06/13/2010 21:33:38	Microso...	6275	Networ...
Information	06/13/2010 21:33:33	Microso...	6275	Networ...
Information	06/13/2010 21:33:28	Microso...	6275	Networ...
Information	06/13/2010 21:33:23	Microso...	6275	Networ...

Event 6275, Microsoft Windows security auditing.

General | Details

Network Policy Server discarded the accounting request for a user.
Contact the Network Policy Server administrator for more information.

User:
Security ID: N/A SID

Log Name: Security
Source: Microsoft Windows security
Event ID: 6275
Level: Information
User: N/A
OpCode: Info

Logged: 06/13/2010 21:33:38
Task Category: Network Policy Server
Keywords: Audit Failure
Computer: server01.traversalabs.com

Fail-No Client Defined in RADIUS for this Authenticator

Network Policy and Access Services 2,407 Events (!) New events available

2,407 Events

Level	Date and Time	Source	Event ID	Task C...
Error	06/13/2010 21:20:49	NPS	13	None
Error	06/13/2010 21:20:44	NPS	13	None
Error	06/13/2010 21:20:39	NPS	13	None
Information	06/13/2010 21:17:38	Microso...	6275	Networ...
Information	06/13/2010 21:17:33	Microso...	6275	Networ...
Information	06/13/2010 21:17:28	Microso...	6275	Networ...

Event 13, NPS

General | Details

A RADIUS message was received from the invalid RADIUS client IP address 10.0.100.254.

Log Name: System
Source: NPS
Event ID: 13
Level: Error
User: N/A
OpCode:

Logged: 06/13/2010 21:20:39
Task Category: None
Keywords: Classic
Computer: server01.traversalabs.c

Fail-no Radius Connection Policy Match

Network Policy and Access Services 2,441 Events

2,441 Events

Level	Date and Time	Source	Event ID	Task C...
Information	06/13/2010 21:39:59	Microso...	6273	Networ...
Information	06/13/2010 21:39:56	Microso...	6275	Networ...
Information	06/13/2010 21:39:51	Microso...	6275	Networ...

Event 6273, Microsoft Windows security auditing.

General | Details

EAP Type: -
Account Session Identifier: -
Reason Code: 49
Reason: The connection attempt did not match any connection request policy.

Log Name: Security
Source: Microsoft Windows security
Event ID: 6273
Level: Information
User: N/A
OpCode: Info

Logged: 06/13/2010 21:39:59
Task Category: Network Policy Server
Keywords: Audit Failure
Computer: server01.traversalabs.com

Fail-no Radius Network Policy Match

The screenshot displays the Windows Event Viewer interface. At the top, the title bar reads "Network Policy and Access Services 2,443 Events". Below this, a filter icon and "2,443 Events" are shown. A table lists several events, with the first three highlighted. The selected event is expanded to show details.

Level	Date and Time	Source	Event ID	Task C...
Information	06/13/2010 21:43:44	Microso...	6273	Networ...
Information	06/13/2010 21:42:40	Microso...	6273	Networ...
Information	06/13/2010 21:39:59	Microso...	6273	Networ...

Event 6273, Microsoft Windows security auditing.

General | Details

Authentication type: EAP
EAP Type: -
Account Session Identifier: -
Reason Code: 48
Reason: The connection attempt did not match any network policy.

Log Name: Security
Source: Microsoft Windows security
Event ID: 6273
Level: Information
User: N/A
OpCode: Info

Logged: 06/13/2010 21:43:44
Task Category: Network Policy Server
Keywords: Audit Failure
Computer: server01.traversalabs.com

Captures Isn't All

- So, where can you look to troubleshoot if the captures don't tell the whole story?
 - Look at RADIUS logs
 - Event Viewer in W2K0/3/8
 - Look at switch logs
 - Look at client Logs
 - Event Viewer

Network Access Security – It's Broke, Now What?

Thank You for Attending!

Jeffrey L Carrell
Network Security Consultant
jeff.carrell@networkconversions.com

www.thenetworksandbox.com

