

# INDEX

## Symbols

---

.dll files, Cisco Trust Agent host requirements, 65  
.inf files, Cisco Trust Agent host requirements, 65

## Numerics

---

### 802.1X authentication

- Cisco Trust Agent hosts, 59
- controlled/uncontrolled ports, 96
- EAP data frames, 99
- EAPoL
  - addressing*, 99
  - protocol message exchange*, 98
- integration issues
  - default operation*, 107–108
  - Guest-VLAN*, 108–109
  - IP telephony*, 109–111
  - management utilities*, 111–113
  - providing for supplemental authentication techniques*, 113–114
- NAC-L2-802.1X
  - EAP-FAST*, 116
  - posture validation*, 114–115
- protocol messages, 98
- RADIUS
  - attributes*, 100–102
  - EAP negotiation*, 102
  - end-to-end EAP*, 103–104
- supplicants, NAC-enabled, 115

### 802.1X Framework

- authentication server, 97
- authenticators, 95–96
- default security, 96–97
- supplicants, 94–95, 97

## A

---

- accounting, leveraging authenticated identity, 117–118
- ACLs (access control lists)
  - intercept ACLs, 127
  - NAC enforcement, 47–48
  - policy enforcement, 133
- ADFs (attribute definition files), 65, 169
- agentless auditing, 31, 33
- agentless hosts, 84, 134–135
- Altiris, 82
- APTs (application posture tokens), health
  - classification states, 26–27
- arbitrary information, collecting from hosts, 30
- architecture of CTA (Cisco Trust Agent), 57–60
  - functions, 58
  - plug-ins, 58
  - services, 57
- ARP (Address Resolution Protocol) inspection, 126–127
- assets, protecting, 205–206
- attribute operations, 30
- attributes of RADIUS for 802.1X, 100–102
- audit servers, 9, 82
- auditing NAHs, 44, 46
- authentication
  - EAP, 35
    - successful authentication*, 47
  - EAP-FAST, 116
- authentication server (802.1X), 97
- authenticators, 95–96
  - EAPoUDP, 126
  - NAC-L2-IP, 126
- authorization, 85, 105
  - GAME, 37
  - HCAP, 36
  - RCAs, 87
  - VLAN assignment, 106
- AVPs for VLAN assignment, 106

## B-C

---

### benefits of NAC, 7

#### Cisco Clean Access, 4, 206

#### Cisco Secure ACS, 76–77, 80

#### Cisco Trust Agent, 9, 132

- 802.1X authentication, 59

- components of, 57

- EAP, identity authentication, 60

- functions of, 58

- logging capabilities, 62

- operating system support, 62–63

- plug-ins, 58

  - functionality of*, 64

- services, 57

#### Cisco Works Interface Configuration Manager, 152

#### Cisco-PEAP, 132

#### client-side protocols, 36

#### CNPC (Cisco Network Profile Collector), 152

#### collecting host credentials

- arbitrary information, 30

- host credential information, 28–30

#### communication plans for NAC Framework deployment to users, 195–196

#### communications protocols

- client-side, 36

- EAP, 35

  - successful authentication*, 47

- EAPo802.1X, 36

- EoU, 36

- GAME, 37

- HCAP, 36

- RADIUS, 36

- server-side, 36

#### company asset management, example NAC policy, 210

#### compliance enforcement process, 13–16, 206

#### conducting proof of concept, 160–161

#### configuring NAP authentication, 78

#### controlled ports (802.1X), 96, 111

#### corporate security policy, defining, 145–149

- acceptable use policy, 147

- incident-handling policy, 149

- information security, 146

- network access control policy, 147

- security management policy, 148–149

#### cost considerations for NAC Framework

##### deployment, 161–163

#### credentials, 56

- ADFs, 169

- arbitrary information, collecting from hosts, 30

- attributes for posture agents, 64–65

- chaining, 60

- collecting from hosts, 28–30

- defining for NAC Policy Framework, 167–172

- validating, EAPoUDP, 128–129

#### CSA (Cisco Security Agent)

- automatic Cisco Trust Agent deployment, 69

- benefits of NAC Framework implementation

  - automatic Cisco Trust Agent*

  - deployment*, 69

  - Cisco Trust Agent protection*, 66

  - NAC state awareness*, 67

  - Trusted QoS*, 67–68

#### CS-MARS (Cisco Secure Monitoring, Analysis and Response System), detecting malicious behavior, 207

#### customized shared resources, example NAC policy, 212

## D

---

#### data restriction, example NAC policy, 212

##### defining

- corporate security policy, 145–149

  - acceptable use policy*, 147

  - incident-handling policy*, 149

  - information security policy*, 146

  - network access control policy*, 147

  - security management policy*, 148–149

- network admission policy, 164–167, 169–179

  - content caching*, 177–178

  - credentials*, 167, 169–172

  - default network access*, 176

  - identity authorization*, 172–174

  - isolation*, 175

  - NAHs*, 178–179

  - network virtualization*, 175

  - patch management*, 176–177

#### deployment scenarios, 16–18

**design phase of NAC Framework lifecycle**

- high-availability considerations, 185–188
  - Cisco Secure ACS load balancing*, 187–188
  - external PVS failover*, 187
  - IOS RADIUS server failover*, 186
- network admission policy, defining, 164–167, 169–179
  - content caching*, 177–178
  - credentials*, 167–172
  - default network access*, 176
  - identity authorization*, 172–174
  - isolation*, 175
  - NAH definition*, 178–179
  - network virtualization*, 175
  - patch management*, 176–177
- scalability considerations, 180–185
  - ACS database replication and synchronization*, 183
  - calculations, performing*, 184–185
  - dispersal of NADs/ACs*, 180
  - NAC timers*, 182–183
  - number of hosts and users*, 181
  - protocol authorization rates*, 182

**detecting**

- malicious behavior, 207–208
- noncompliant hosts, 6–7

**developing migration strategy, 161****development of NAC technology, 4–5****device authorize statements, 136****devices, authenticators, 95–96****DHCP-Snooping, 126–127****documenting current infrastructure, 151–158****E****EAP (Extensible Authentication Protocol), 35**

- data frames, 99
- negotiation, 102
- of Cisco Trust Agent hosts, 60
- successful authentication, 47

**EAP-FAST (EAP-Flexible Authentication via Secure Tunneling), 116, 209****EAPo802.1X, 36****EAPoL (EAP over LAN), 802.1X**

- exchange addressing components, 99
- supplicant-initiated authentication exchange, protocol messages, 98

**EAPoUDP (Extensible Authentication Protocol over User Datagram Protocol), 36, 125**

- agentless hosts, 134–135
- authenticators, 126
- bypasses, 138
- Cisco Trust Agent, 132
- credential validation, 128–129
- PEAPv1, 132
- policy enforcement, 133
- posture validation triggers, 125–127
- RADIUS, 129–132
- session initiation, 127–128
- status query techniques, EAP-SQ, 134
- URL redirect, 133
- voice integration
  - PVID*, 135–136
  - summary of*, 137–138
  - trust agent disappearing*, 136–137
  - VVID*, 135–136

**EAP-SQ (EAP-Status-Query), 134****EAP-TLV (EAP-type-length value), 209****end-to-end EAP, 103–104****enforcing policy compliance, 206**

- enforcement actions, specifying, 86–88

**enterprise security policies, planning, 83****estimating**

- hardware costs for NAC Framework deployment, 162
- installation/operation costs for NAC Framework deployment, 162–163
- software costs for NAC Framework deployment, 161–162

**evaluating posture policies, 83–84****examples of NAC policies, 210–211**

- company asset management, 210
- customized shared resources, 212
- data restriction, 212
- physical identification enforcement, 210
- regulatory compliance enforcement, 211
- roles-based provisioning, 211

**exception lists, 138****extended ACLs, 47****external posture validation servers, 80–81**

## F-G

---

### **functionality**

- of Cisco Trust Agent, 58
- of posture agent plug-ins, 64–65

**GAME (Generic Authorization Message Exchange), 37, 208**  
**Guest-VLAN (802.1X), 108–109**

## H

---

**hardware costs for NAC Framework deployment, estimating, 162**

**HCAP (Host Credential Authorization Protocol), 36, 208**

**health classification states (APTs), 26–27**

**healthy hosts, 3**

**high-availability considerations for NAC Framework deployment, 185–188**  
Cisco Secure ACS load balancing, 187–188  
external PVS failover, 187  
IOS RADIUS server failover, 186

**HIPS (host-based IPS), detecting malicious behavior, 207**

### **hosts**

- agentless, 134–135
- credential information, collecting, 28–30
- HAHs, auditing, 44–46
- NAHs
  - agentless auditing, 31–33*
  - exception handling, 49*
  - static exemptions, 31*

## I-L

---

**identifying NAC solution objectives, 150–151**

**Identity-Based Networking Services, 205**

**implementation phase of NAC Framework lifecycle, 188–195**

- communication to users, 195–196
- migration strategies, 189–195

**incident-handling policy, defining, 149**

**information security policy, defining, 146–147**

**installation/operation costs for NAC Framework deployment, estimating, 162–163**

### **integration issues for 802.1X**

- default operation, 107–108
- Guest-VLAN, 108–109
- IP telephony, 109–111
- management utilities, 111–113
- providing for supplemental authentication techniques, 113–114

**integration strategy, identifying, 158**

**intercept ACLs, 127**

**interesting traffic (exception lists), 138**

**interoperability between NAC framework model hosts/users, 208**

**IP addresses, whitelisting, 85**

**IP telephony (802.1X), 109–111**

**leveraging authenticated identity, 117–118**

**Linux host posture plug-in, 63**

**load balancing, Cisco Secure ACS, 187–188**

**logging capabilities on Cisco Trust Agent, 62**

## M

---

**MAB (MAC Authentication Bypass), 49**  
whitelisting, 84

**MAC addresses, whitelisting, 85**

**malicious behavior, detecting, 207–208**  
**management utilities as 802.1X integration concern, 111–113**

**McAfee Policy Enforcer, 82**

### **migration strategies**

- developing, 161
- for NAC Framework deployment, 189–195

## N

---

**NAC (Network Admission Control), 145**

- enforcement, 47
- layer 3 operations, EAPoUDP, 125–126
- policies, examples of, 210–212
- posture agents, 55–56

via ACLs, 47–48

via posture plug-ins, 48

#### **NAC Appliance model, 205–206**

#### **NAC Framework, 205**

agentless hosts, 84

APTs, health classification states, 26–27

authorization, 23, 85

Cisco Secure ACS support, requirements,  
12–13

Cisco Trust Agent support, requirements, 13

components, 8–9

deployment scenarios, 16–18

enforcement actions, 86–88

host credential information, 28–30

*arbitrary information, collecting, 30*

modes of operation, 33–34

PDIOO lifecycle

*design phase, 164–188*

*implementation phase, 188–196*

*operation and optimization phases, 197*

*planning phase, 150–163*

*preparation phase, 145–149*

PDIOO lifecycle phases, 144

posture validation flow, 23–26

posture validation servers, 75

protocols, 208–209

release 1.0, 4

requirements, 206

*router support, 10*

*switch support, 11*

*VPN concentrator support, 11*

*wireless support, 12*

software compliance enforcement process,  
13–16

Cisco Trust Agent, 9

NADs, 9

policy servers, 9

vendors

*ADFs, 65*

*interoperability, 208*

with external policy servers, 80–81

#### **NAC-enabled 802.1X supplicants, 115**

#### **NAC-L2-802.1X, 34, 114**

EAP-FAST, 116

periodic posture reassessment, 115

posture validation, 41, 44

#### **NAC-L2-IP, 34**

authenticators, 126

exception lists, 138

policy enforcement, ACLs, 133

posture validation triggers, 127

#### **NAC-L2-IP/NAC-L3-IP posture validation, 39–41**

#### **NAC-L3-IP, 34**

#### **NADs (network access devices), 8–9**

#### **NAHs (NAC agentless hosts), 4**

agentless auditing, 31–33, 44–46

defining for NAC Framework, 178–179

exception handling, 49

static exemptions, 31

#### **naming conventions, importance in network**

**admission policies, 174**

#### **NAPs (network access profiles), 77**

#### **network access control policy, defining, 147**

#### **network admission control models, 205**

#### **NIPS (network-based IPS), detecting malicious behavior, 207**

#### **noncompliant hosts**

detecting, 6–7

network, accessing, 5–6

#### **nonresponsive hosts, 84, 134–135**

## **O**

#### **operating system support on Cisco Trust Agent, 62–63**

#### **operation and optimization phases of NAC Framework lifecycle, 197**

#### **operational strategy, identifying, 159–160**

#### **out-of-band protocols, 37**

## **P**

#### **PACLs (port access control lists), 47**

#### **PBACLs (policy-based ACLs), 48**

#### **PDIOO phases of NAC Framework lifecycle**

design phase

*high-availability considerations, 185–188*

*network admission policy, defining,  
164–179*

*scalability considerations, 180–185*

- implementation phase, 188–195
  - communication to users*, 195–196
  - migration strategies*, 189–195
- operation and optimization phases, 197
- planning phase
  - cost considerations*, 161–163
  - current infrastructure, documenting*, 151–158
  - integration strategy, identifying*, 158
  - migration strategy, developing*, 161
  - objectives, identifying*, 150–151
  - operational strategy, identifying*, 159–160
  - POC, conducting*, 160–161
- preparation phase, defining corporate security policy, 145–149
- PDPs (policy decision points), 56**
- PEAPv1, 132**
- Perfigo CleanMachines, 4**
- performing CS ACS scaling calculations for NAC deployment, 184–185**
- physical identification enforcement, example NAC policy, 210**
- planning posture policies**
  - enterprise security policies, 83
  - policy evaluation, 83–84
  - posture rules, 83
- planning phase of NAC Framework lifecycle**
  - cost considerations, 161–163
  - current infrastructure, documenting, 151–158
  - integration strategy, 158
  - migration strategy, developing, 161
  - objectives, identifying, 150–151
  - operational strategy, 159–160
  - POC, conducting, 160–161
- plug-ins**
  - for Cisco Trust Agent, 58
  - for posture agents, 61–62
    - functionality*, 64
    - functionality of*, 65
    - NAC enforcement*, 48
- POC (proof of concept), conducting, 160–161**
- policeman analogy of NAC enforcement characteristics, 203–204**
- policies**
  - attribute operations, 30
  - compliance, enforcing, 86–88, 206
  - evaluating, 83–84
  - examples of, 210–211
    - company asset management*, 210
    - customized shared resources*, 212
    - data restriction*, 212
    - physical identification enforcement*, 210
    - regulatory compliance enforcement*, 211
    - roles-based provisioning*, 211
  - posture policies, 83
  - posture validation rules, 79
- policy evaluation points, 76**
- policy rules, 83**
- policy servers, 9**
- posture agents, 55–56**
  - Cisco Trust Agent
    - 802.1X authentication*, 59
    - architecture*, 57
    - EAP, identity authentication*, 60
    - functions of*, 58
    - logging*, 62
    - operating system support*, 62–63
    - plug-ins*, 58
    - services*, 57
  - credential attributes, 64–65
  - functions performed by, 56
  - plug-ins, 61–62
    - functionality*, 64
    - functionality of*, 65
- Posture notification TLV, 132**
- posture plug-in actions, 87**
- posture policy planning**
  - enterprise security policies, 83
  - policy evaluation, 83–84
  - posture rules, 83
- Posture TLV, 132**
- posture validation process, 8, 23–26, 77–79**
  - NAC-L2-802.1X, 41, 44
    - periodic posture reassessment*, 114–115
  - NAC-L2-IP/NAC-L3-IP, 39, 41
- posture validation servers, 75**
  - audit servers, 82
  - external, 80–81
  - policy evaluation points, 76
- posture validation triggers, 125–126**
  - ARP inspection, 126–127
  - DHCP-Snooping, 126–127
  - intercept ACLs, 127
  - NAC-L2-IP, 127

**preparation phase of NAC Framework lifecycle, 145–149**

- corporate security policy, defining
  - acceptable use policy, 147*
  - incident-handling policy, 149*
  - information security policy, 146*
  - network access control policy, 147*
  - security management policy, 148–149*
- corporate security policy, defining, 145–149

**prioritizing NAC solution objectives, 150****progression of NAC technology, 4–5****protecting assets, 205–206****protocol messages for 802.1X EAP exchange, 98****PVID (Port VLAN Identifier), 135–136**

## Q-R

**QualysGuard appliance, 82****RACLs (router access control lists), 48****RADIUS (Remote Access Dial-In User Service), 36**

- attributes for 802.1X, 100, 102
- authenticated identity, leveraging, 117–118
- EAP
  - end-to-end, 103–104*
  - negotiation, 102*
- EAPoUDP, 129–132

**RADIUS-Access-Request packets, 100****RCAs (RADIUS Authorization Components), 87****redirection, 169****regulatory compliance enforcement, example****NAC policy, 211****remediation, 3****requirements**

- for NAC Framework adoption, 206
- for NAC Framework solution, 10
  - Cisco Secure ACS support, 12–13*
  - Cisco Trust Agent support, 13*
  - router support, 10*
  - switch support, 11*
  - VPN concentrator support, 11*
  - wireless support, 12*

**revalidation timers, 40, 44****roles-based provisioning, example NAC policy, 211**

## S

**sample migration strategies for NAC Framework deployment, 189–195****scalability considerations for NAC Framework deployment, 180–183, 185**

- ACS database replication and
  - synchronization, 183
- calculations, performing, 184–185
- dispersal of NADs/ACSs, 180
- NAC timers, 182–183
- number of hosts and users, 181
- protocol authorization rates, 182

**security management policy, defining, 148–149****selecting posture token, 83–84****self-defending network technologies, 207****server-side protocols, 36****services within Cisco Trust Agent, 57****software**

- compliance enforcement process, 13–16
- cost of, estimating for NAC Framework
  - deployment, 161–162

**specifying enforcement actions, 86–88****SPT (system posture token), 26–27****standard ACLs, 47****static exceptions, 49****static exemptions for NAHs, 31****supplicants, 94–97****NAC-enabled, 115****support strategy, defining, 160****surveying current network, 151–158**

## T-U

**TLV file format, 132****Trend Micro OfficeScan solution, 81****trust agent disappearing, 136–137****Trusted QoS, 67–68****uncontrolled ports (802.1X), 96, 111****URL redirect, 133**

## V-W-X-Y-Z

---

**VACLs (VLAN access control list), 48**

**validation**

credential validation, EAPoUDP, 128–129

posture validation triggers, 125–126

*ARP inspection, 126–127*

*DHCP-Snooping, 126–127*

*intercept ACLs, 127*

*NAC-L2-IP, 127*

**VLAN assignment, 106**

**VSAs (vendor-specific attributes), 77**

**VVID (Voice VLAN Identifier), 135–136**

**whitelisting, 84**