UPnP Forum and Gateway committee overview

March 15, 2010

Mika Saaranen – Nokia

UPnP Gateway Chair

Mark Baugher – Cisco

UPnP Gateway Vice-Chair

Introduction

- This is a public presentation of the the UPnP Forum's Gateway work
- The contents of this presentation are
  - UPnP Forum overview
  - Foundation of UPnP technology
  - Overview of UPnP InternetGateway v1 features
  - Overview of UPnP InternetGateway v2 features
    - NAT Traversal changes & IPv6 Firewall Control
    - DeviceProtection v1 Security Service (for all DCPs)
    - Updates to the UDA IPv6 Annes
  - Detailed technical presentation of all UPnP IGD:2 new features are in the "backup" section of this presentation

What is UPnP Technology

1. UPnP Technology is an open international ISO/IEC standard for device & service discovery & control of devices on an IP-based home network – supporting interoperability independent of underlying physical network technology.
2. UPnP standards are adopted and used by many global standards organizations including DLNA, Broadband Forum, OpenIPTV Forum and CEA.
3. The UPnP Forum has 606 certified device implementations from 66 companies. Additionally, DLNA has certified more than 6,000 products.
4. Hundreds of millions of UPnP devices are already deployed (internet gateways, TVs, PCs, game consoles, mobile phones, Blu-ray players, and others)

    ABI Research reports DLNA deployed devices: 250 million in 2009, and projects about 1 billion in 2012, about 2 billion in 2014

Diversity of UPnP Vendors & Products

Game consoles

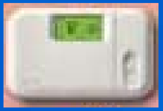
Networked Storage

Blu-ray Players

Wireless printers

DVD Players

Cell Phones



Thermostats

Routers Gateways

Lighting Control

A/V Receivers

Multi-room Audio

DTVs

Cameras

Digital Media Adapters

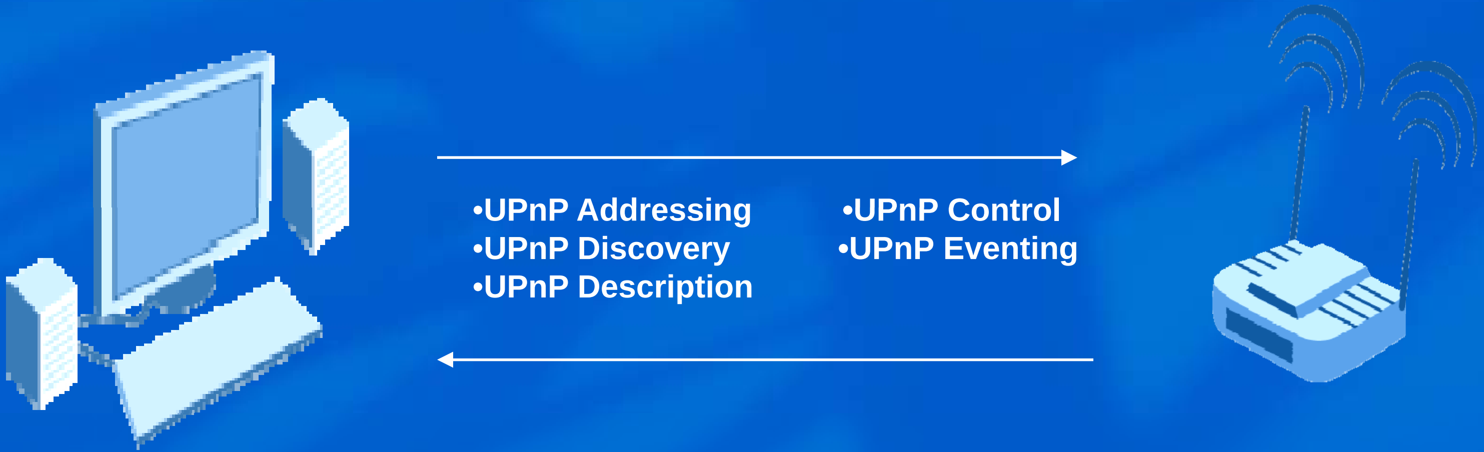
1. Acer Aspire Laptop PC series
2. Buffalo HS-DS Network Attached Storage (NAS) series
3. Canon Digital Camera DS585784
4. Cisco-Linksys Network Media Hub
5. Corega 802.11N AP/Router
6. Denon iPod/Networking Client dock ASD-3W
7. Digeo MOXI HD DVR
8. Epson All-In-One Printers
9. HP Photosmart Plus All-in-One
10. Hitachi LCD TV UT Series
11. I-O Data AVeL LinkPlayer AV-LS300DW DVD Player/Recorder
12. Iomega Home Media Network Hard Drive
13. LG Electronics Media Station and BD Player
14. NEC Valuestar/LaVie PC series
15. ONKYO Receivers
16. Panasonic Blu-ray Disc Recorder DMR-BW730
17. Nokia N95/N85/N78 mobile phones
18. Philips 42PFL9603D/10 Flat TV, NP1100 DMA, Wi-Fi Photo Frame 8FF3WMI
19. Promise Technology Network Attached Storage - SmartStor NS2300N
20. Pioneer Flat Screen TV series and AV Receiver VSX-94TXH
21. Samsung HDTV LN40 Series and SGH-i900 Smart Phone
22. Seagate NAS
23. Sharp AQUOS LC-46RX5 LCD TV
24. Sony Bravia KDL Series HDTV and Playstation 3
25. Sony-Ericsson Mobile Communications C905/C705 mobile phones
26. Thomson TG787g Residential Gateway NAS
27. Toshiba Laptops and REGZA TVs
28. Western Digital NAS
29. Yamaha DSP-AX3900/RX-V3900 AV Player/Receiver
30. Zyxel DMA-1000 Digital Media Adapter and NAS-220

UPnP™ FORUM

UPnP Working Committees

- UPnP protocols are developed in UPnP Working Committees
- There are many past and present WCs including
  - Audio/Video Server and Renderer (referenced by DLNA)
  - Gateway
  - Device Management
  - QoS
  - Remote Access
  - Telephony
  - HVAC
  - Lighting Controls
  - Security Camera
  - Scanner, Printer and many other device controls

What is UPnP?

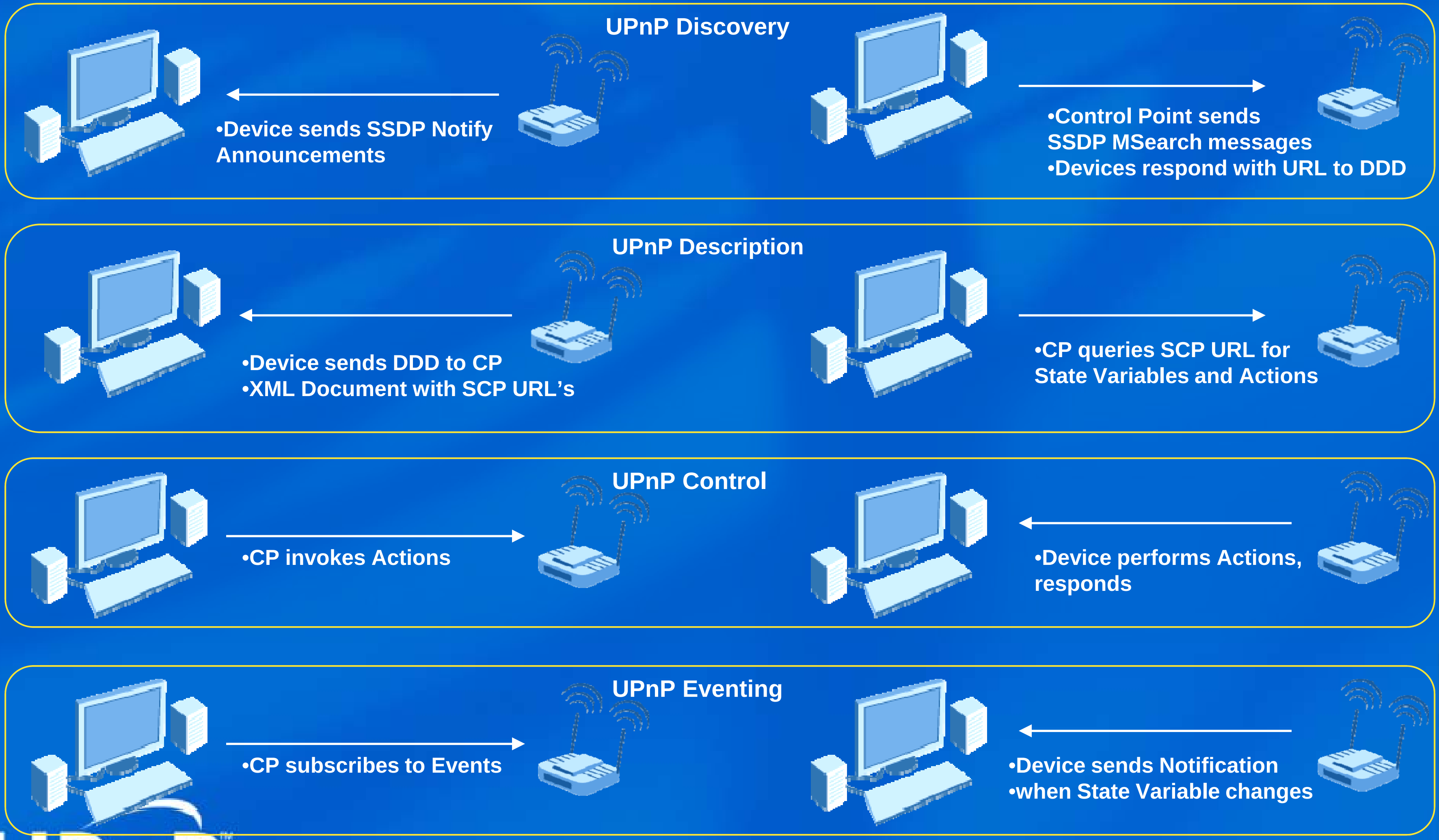


- UPnP Addressing
- UPnP Discovery
- UPnP Description

- UPnP Control
- UPnP Eventing

- UPnP Device Architecture (UDA) defines networking protocol suite for device discovery and control on unmanaged (home) networks
    - Any number of (authorized) Control Points can interact with a device
    - UPnP uses standard web protocols such as IP, TCP, UDP, HTTP Unicast, HTTP Multicast, XML, and SOAP
- Device Control Protocols (DCPs) define the specifics for a given subject area (e.g. A/V, Telephony, QoS, etc.)

UDA Overview



UPnP Discovery

- Device sends SSDP Notify Announcements

- Control Point sends SSDP MSearch messages
- Devices respond with URL to DDD

UPnP Description

- Device sends DDD to CP
- XML Document with SCP URL’s

- CP queries SCP URL for State Variables and Actions

UPnP Control

- CP invokes Actions

- Device performs Actions, responds

UPnP Eventing

- CP subscribes to Events

- Device sends Notification
- when State Variable changes

The Risks of Home Networking

Home networks are vulnerable to malware and war drivers

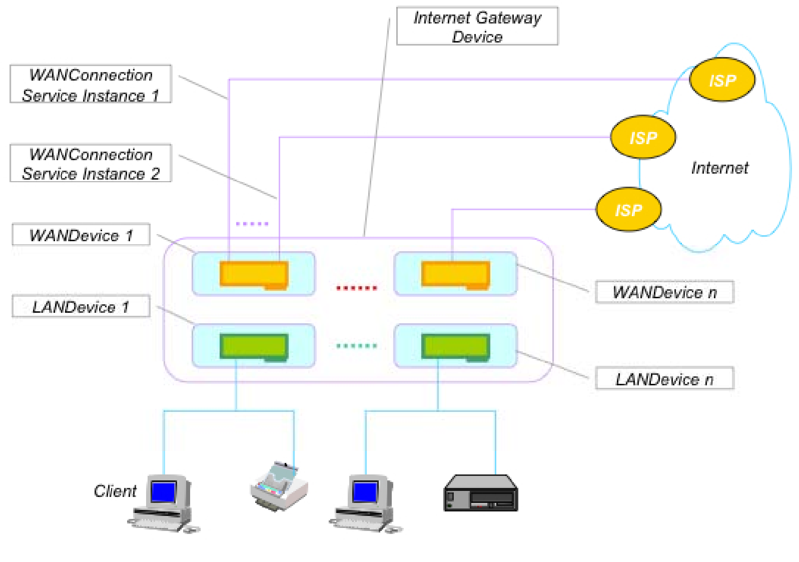


Figure 1: *InternetGatewayDevice* with LAN and WAN Interfaces

The UPnP Forum is developing a device protection service for UPnP IGD and other Device Control Protocols

- Home networks face risks
  - Well-known admin passwords
  - Little authentication of services
  - Viruses are common on home computers
- Malware is biggest threat (viruses, Flash-based attacks)
- War Driving is another

UPnP™ FORUM

Gateway V1 overview

- Manage and configure physical connections e.g. connect or disconnect
- Automatic and seamless configuration of Internet access among networked devices
- Status and events on connections like External IP address
- Control NAT traversal

Security in Gateway V1

- IGD and other UPnP DCPs have had the option of using UPnP Device Security for the past 6 years
  - This is a high-grade security service
  - No significant flaws were found in UPnP Device Security
  - Still, vendors have not chosen to ship Device Security
- The Security Task Force considered the technical factors that might have made deployment so hard
  - These are addressed in UPnP Device Protection

Gateway v2 overview

- Enhanced security by new DeviceProtection service applied to all IGD variables and actions
- Enhanced portmapping by new action giving any free portmapping if requested mapping is not free
  - Policy changes e.g. no infinite portmappings
- New service for controlling IPv6 firewalls
- Clarifications for UPnP IPv6 support

Addressing Security in V2

- Threats: Malicious edits to critical configuration variables
  - DeviceProtection service uses **public** (unauthenticated), **basic** and **admin** (authenticated) access controls
- Risks: Bypassing device admin-level access controls
  - DeviceProtection applies access controls to all vulnerable services and data and uses stronger authentication for admin
- Protection of Assets
  - DeviceProtection allows vendors as well as users to limit access to specific services and data

Security in Gateway V2

- Gateway v2 will use UPnP Device Protection
  - Does not require a third-device as a security console
  - Uses X.509 certificates and SSL/TLS services
  - Uses WiFi Protected Setup means of enrollment
- IGD & other DCPs can use UPnP Device Protection
  - Device Protection is a UPnP service for all DCPs
  - DP provides an extensible authorization framework
- IGD has applied Device Protection to its needs
  - Three-levels of authorization and authentication
    - Admin, Basic and Public

Access Controls in IGD:2

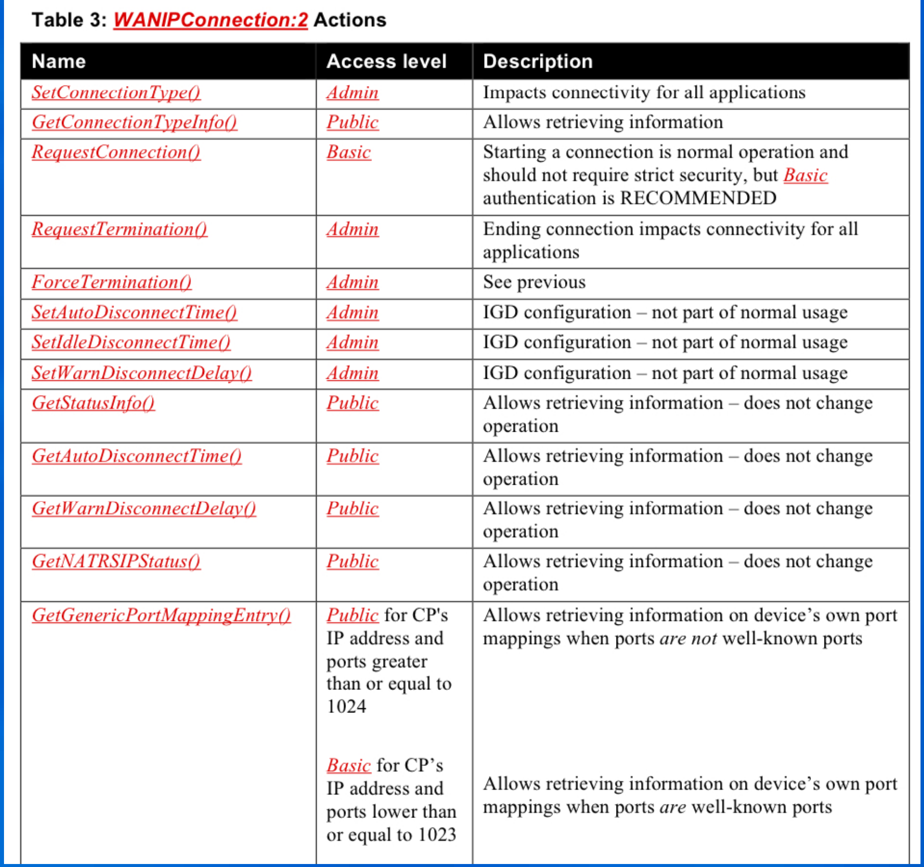


Table 3: *WANIPConnection:2* Actions

Name	Access level	Description
SetConnectionType()	*Admin*	Impacts connectivity for all applications
GetConnectionTypeInfo()	*Public*	Allows retrieving information
RequestConnection()	*Basic*	Starting a connection is normal operation and should not require strict security, but *Basic* authentication is RECOMMENDED
RequestTermination()	*Admin*	Ending connection impacts connectivity for all applications
ForceTermination()	*Admin*	See previous
SetAutoDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetIdleDisconnectTime()	*Admin*	IGD configuration – not part of normal usage
SetWarnDisconnectDelay()	*Admin*	IGD configuration – not part of normal usage
GetStatusInfo()	*Public*	Allows retrieving information – does not change operation
GetAutoDisconnectTime()	*Public*	Allows retrieving information – does not change operation
GetWarnDisconnectDelay()	*Public*	Allows retrieving information – does not change operation
GetNATRSIPStatus()	*Public*	Allows retrieving information – does not change operation
GetGenericPortMappingEntry()	*Public* for CP's IP address and ports greater than or equal to 1024 *Basic* for CP's IP address and ports lower than or equal to 1023	Allows retrieving information on device's own port mappings when ports *are not* well-known ports Allows retrieving information on device's own port mappings when ports *are* well-known ports

Access control is defined

- For all IGD Actions

Three levels of access

- Admin
- Basic
- Public

Better overall security

- Least privilege
- Privilege separation

UPnP™ FORUM

UDA Annex A IPv6 Changes

- IPv6 support in UDA 1.0 and 1.1 evolved with the evolving standard
  - Deprecation of site-local addressing
  - Development of unique local addressing
  - Publication of RFC 3484 address selection policies
- Allow routed home networks using ULAs
  - 802.14.5 uses a 64-bit address means that it cannot be bridged to Wi-Fi, Ethernet, MoCA, or other LANs.
  - Accommodate routed private networks with site-routing without resorting to globally-routable addresses.

Time table

This presentation covers on-going work and may change before publication. Target timeline is:

- WANIPConnection:2 Q4/2010
- DeviceProtection:1 Q4/2010
- IPv6 update and firewall control: Q4/2010

Summary

- IGD:2 introduces two new services:
  - DeviceProtection :1 to enable authentication and access control
  - WANIPv6firewallControl:1 for controlling IPv6 firewalls
- There is new and enhanced portmapping experience with WANIPConnection:2 service
- A number of policy changes that improves security and resource usage
- This presentation covers on-going work and may change before publication.

Technical details

WANIPCONNECTION:2

Key Use Cases

- Use case #1 Add portmapping
  - User has an application that needs to be contacted from the internet
  - Usually, no user interaction is needed: Application uses IGD control point to make required portmappings (or a UI can be used)
  - It is possible to get any free portmapping or request a specific one
- Use case #2 – delete portmappings
  - Applications may remove portmappings automatically or user may use UI to delete specific mappings
  - It is possible to remove single items or ranges
- Use case #3 – find out existing portmappings
  - Control point UI allows user to retrieve list of portmappings for diagnostic or other purposes

List of Key changes Features - actions

- DeletePortMappingRange() allows removing a range of portmappings
- GetListOfPortmappings() allows retrieving a list of existing portmappings.
- AddAnyPortMapping() allows requesting specific external port and if the port is not free the gateway assign a free port. Policy how to determine the assigned port is left to vendors

List of Key changes Features New – state variables

- SystemUpdateID is used to track changes in NAT portmappings
- A_ARG_TYPE_MANAGE is a parameter used in new actions
- A_ARG_TYPE_PortListing is a data structure used to return a list of portmappings

List of Key changes Features – policy changes

- PortmappingLeaseTime can have values between 1 to 604800 seconds
- If control point uses value 0 to indicate infinite lease time mapping, it is required that gateway uses maximum value instead
- In IGD there is access control feature introduced.
- If a Control point has not been authenticated and authorized as defined in the DeviceProtection service, control points may request portmappings only for their own IP address
- If a Control point has not been authenticated and authorized, the External port value must be >1023
- It is not possible to require that ExternalPort must be equal to InternalPort

DeviceProtection:1

Vic Lortz (Intel) chair of UPnP Gateway security Task Force

Mika Saaranen (Nokia), Chair of UPnP Gateway committee

Background

- Ease of use is generally at odds with secure use
  - People find that passwords and other authentication methods are a challenge to manage on home networks
  - Easily defining authorizations is also a big challenge
  - There needs to be user involvement in both
- UPnP DeviceProtection work was initiated to create a security solution that
  - Is easy to use and can be attached to other mechanisms namely Wifi Protected setup
  - Has industry support
  - Provides adequate level of security
  - Supports legacy services

Basic Security Requirements

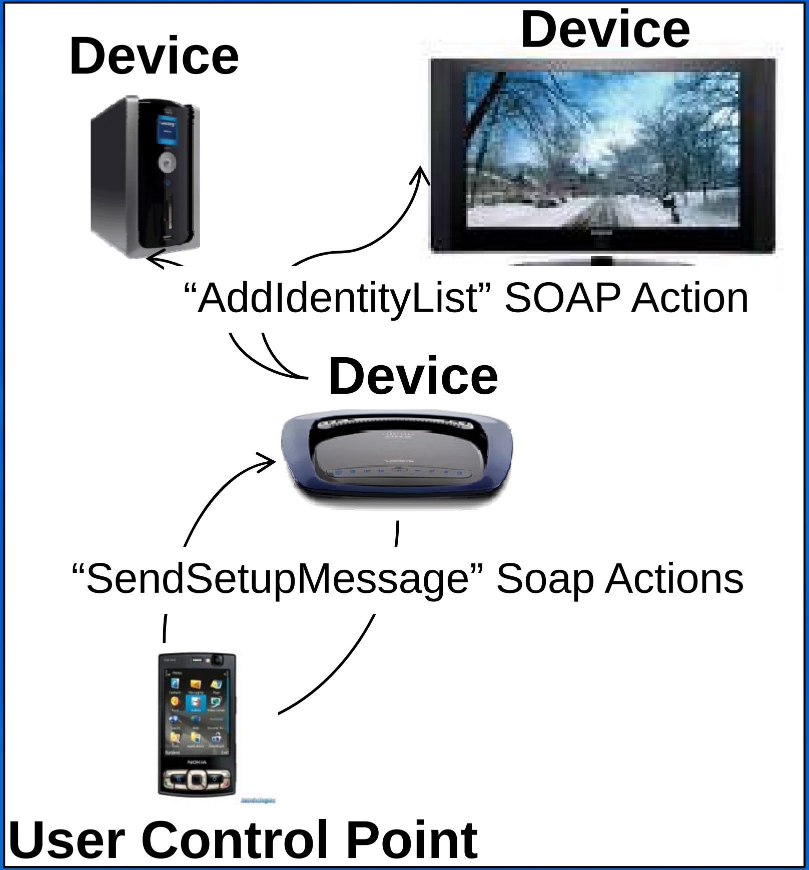
1. Simple to understand and use
2. Mutual authentication
3. Access control
4. Privacy
5. Align with widely-supported security mechanisms
6. Decentralized trust model
7. Both Device Identities and User Identities

Device Protection Properties

1. Trust based on physical proximity and access
   - Such as reading a PIN
   - Pushing a button,
   - NFC touch, etc.
2. Bootstraps strong cryptographic secrets
   - X.509 Server and Client certificates (2048 RSA)
   - Password-based User login uses PKCS#5, protected by HTTPS
3. Role-based per-device access control lists

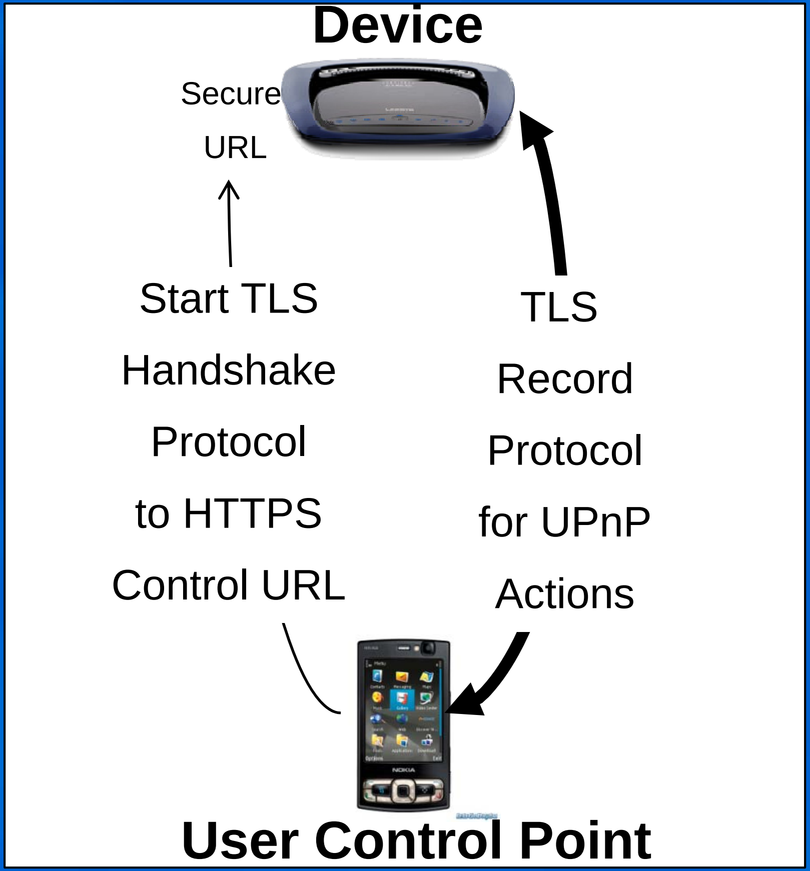
Note: data plane protection is out of scope

Trust Boostrapping by Introduction


Device
Device
"AddIdentityList" SOAP Action
Device
"SendSetupMessage" Soap Actions
User Control Point

1. Pair-wise introduction
   A. PIN-based, run once
   B. Establishes trust in self-signed certs of both Device and CP
   C. Successful introduction establishes default Role for CP
2. "Gossip" introduction
   A. With AddIdentityList(), authorized CPs propagate other CP Identities to devices on network
   B. "Gossip" model only propagates Identity information, not authorization

Securing the Control Plane



Device

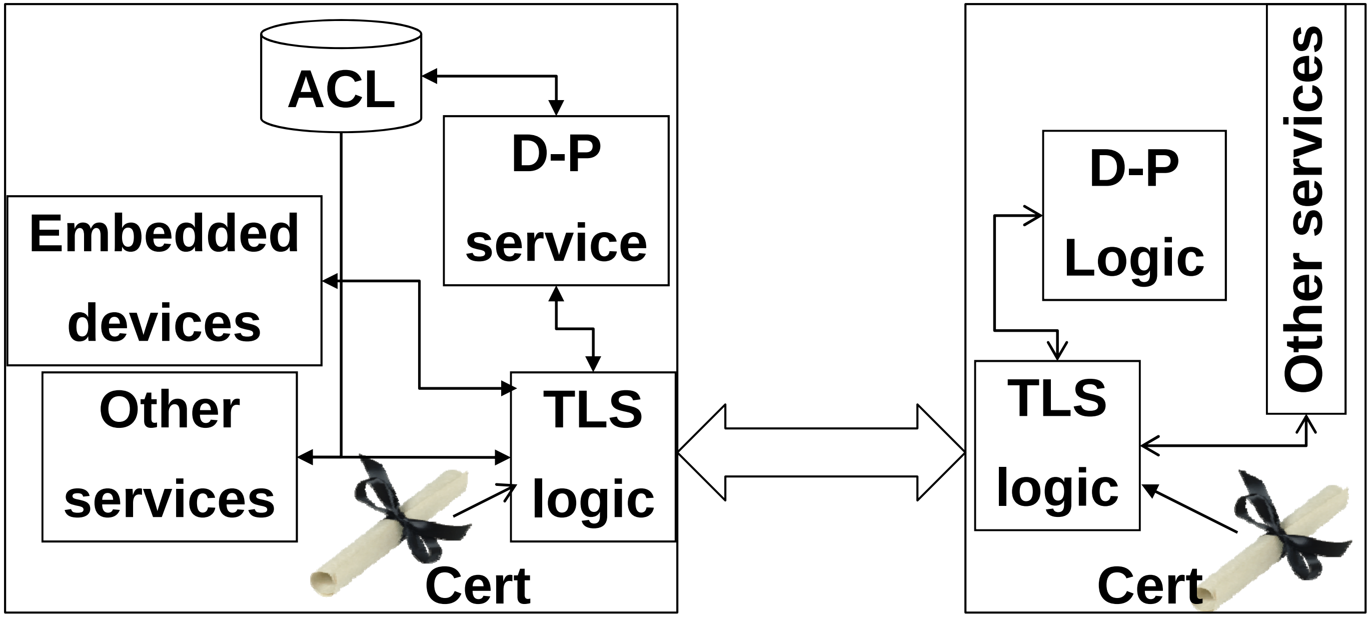
Secure URL

Start TLS Handshake Protocol to HTTPS Control URL

TLS Record Protocol for UPnP Actions

User Control Point

D-P Functional Block Diagram



DEVICE

CONTROL POINT

IGD User Experience Scenario

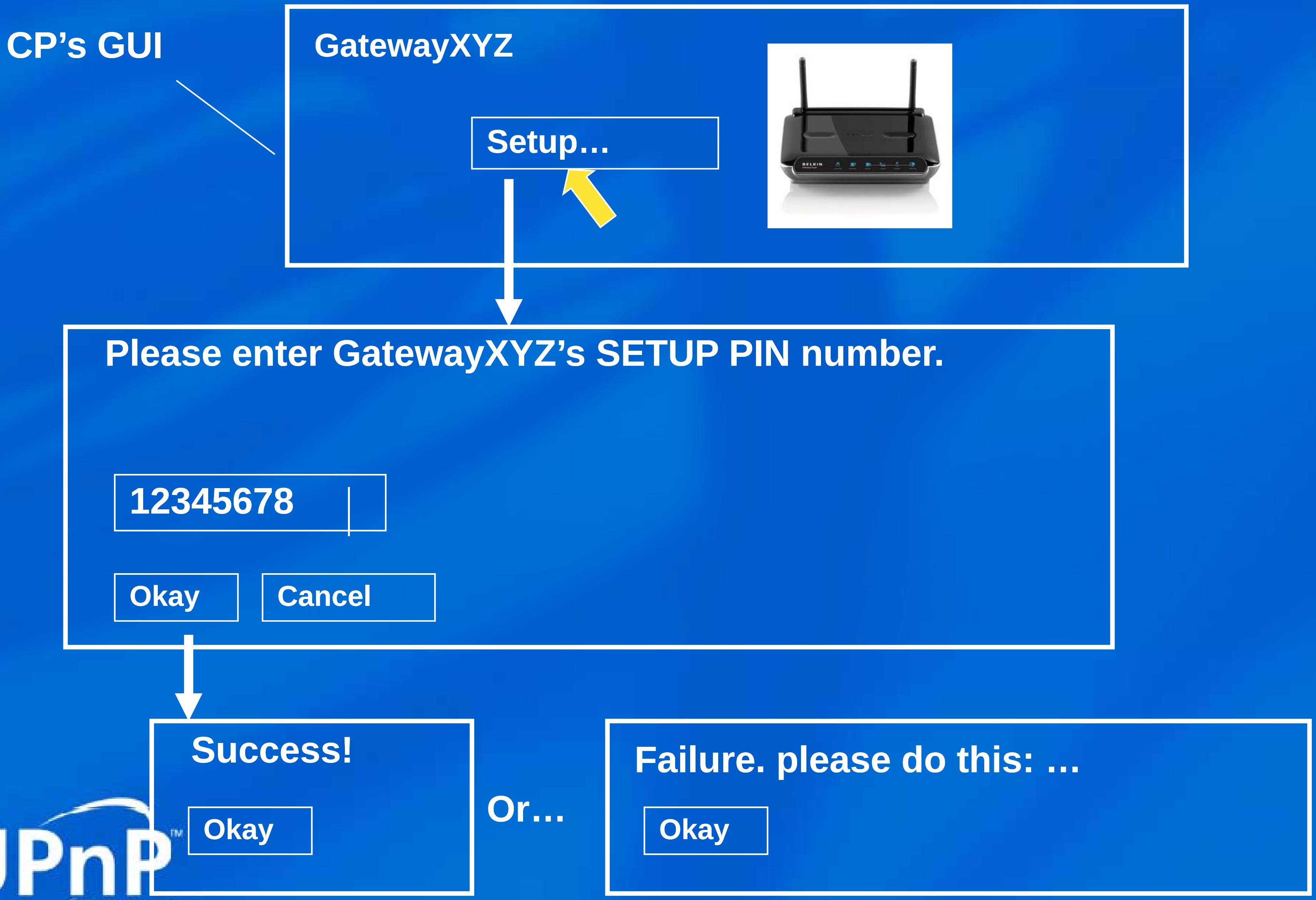
IGD Scenario

Control Point

IGD

- CP on laptop and IGD are already connected to an IP network (may be wired or wireless)
- User introduces CP to IGD (IGD and CP exchange certs)
- IGD automatically assigns new CP a default role of “Basic”
- Basic is recommended, but Device MAY have different policy
- Gaining Admin rights to a device or asserting a User identity requires login with username/ password

Example Setup UI Flow



CP’s GUI

GatewayXYZ

Setup…

Please enter GatewayXYZ’s SETUP PIN number.

12345678

Okay

Cancel

Success!

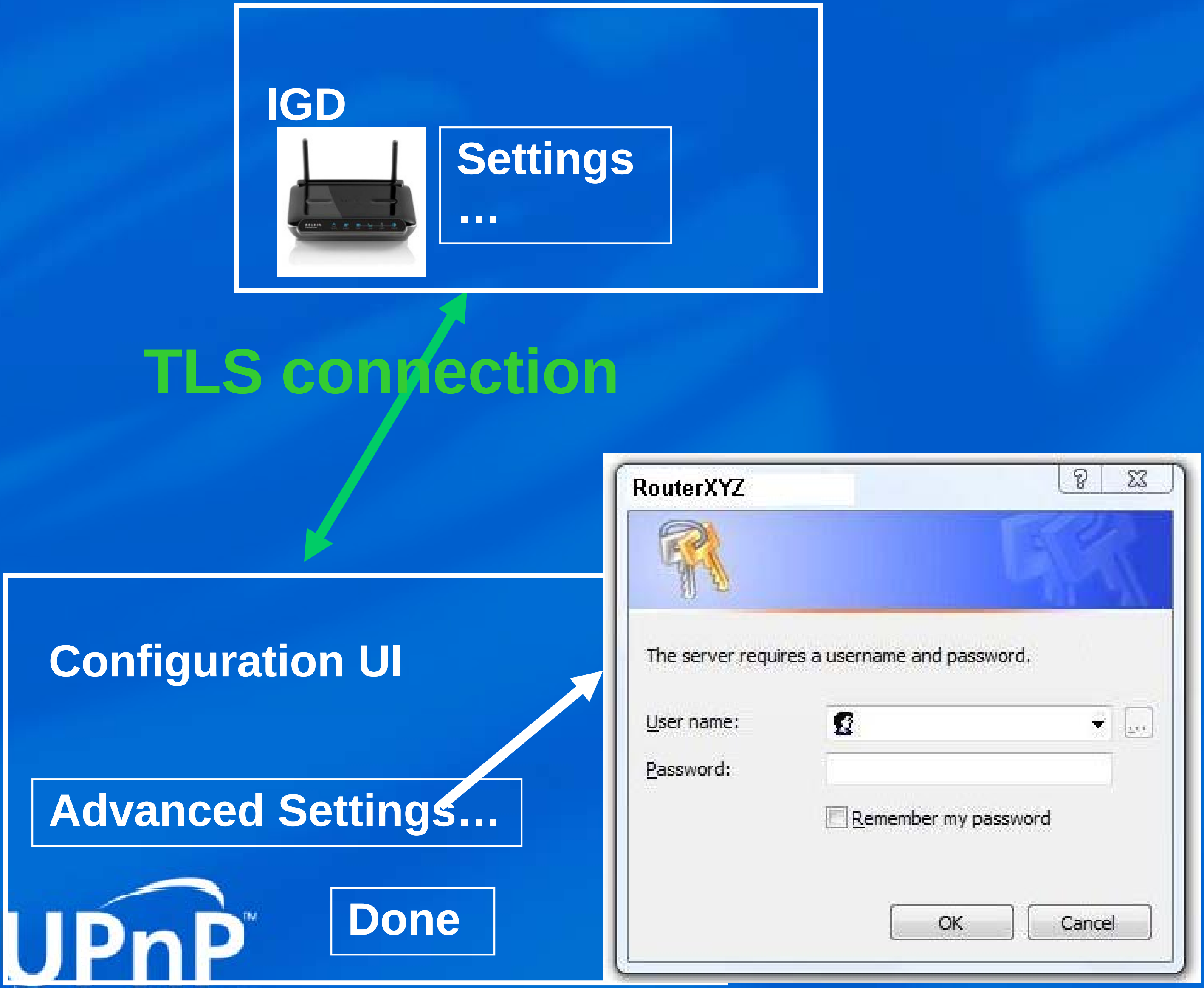
Okay

Or…

Failure. please do this: …

Okay

Administrator Login (rarely needed)



IGD

Settings …

TLS connection

Configuration UI

Advanced Settings…

Done

RouterXYZ

The server requires a username and password.

User name:

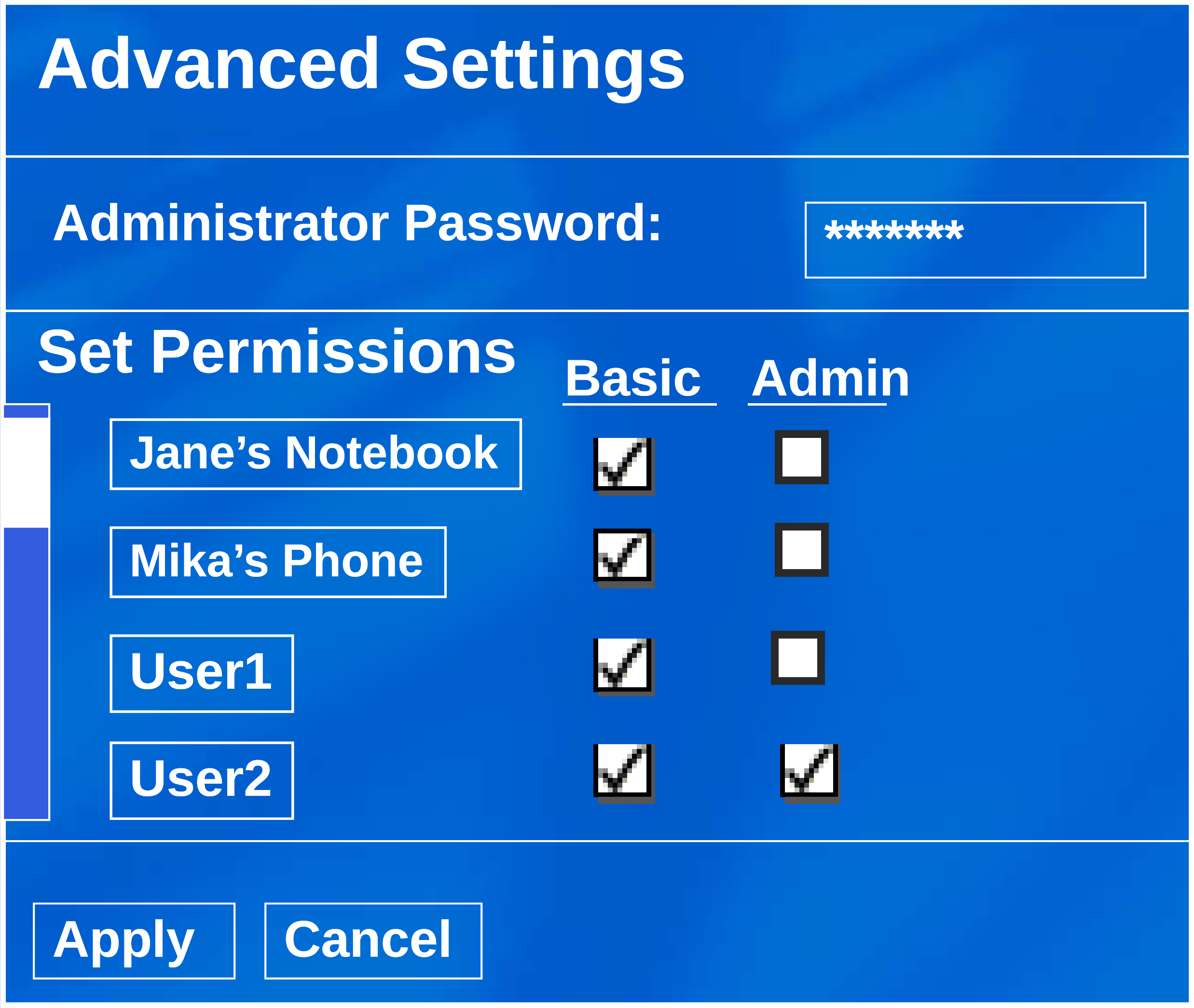
Password:

□ Remember my password

OK

Cancel

Concept UI of Administrative CP



Advanced Settings

Administrator Password: ********

Set Permissions

	Basic	Admin
Jane’s Notebook	☑	☐
Mika’s Phone	☑	☐
User1	☑	☐
User2	☑	☑

SOAP Actions & Roles for the D-P Service

- *SendSetupMessage() [Public]*
- *GetSupportedProtocols() [Public]*
- *GetAssignedRoles() [Public]*
- *GetRolesForAction() [Basic or Admin]*
- *GetUserLoginChallenge() [Basic or Admin]*
- *UserLogin() [Basic or Admin]*
- *UserLogout() [Basic or Admin]*
- *GetACLData() [Basic or Admin]*
- *AddIdentityList() [Basic or Admin]*
- *RemoveIdentity() [Admin-only]*
- *SetUserLoginPassword() [Basic or Admin]*
- *AddRolesForIdentity() [Admin-only]*
- *RemoveRolesForIdentity() [Admin-only]*

Summary

1. CPs and Devices authenticate each other using certificates, users of shared CPs can also authenticate with Username/password over TLS
   1. Device uses ACL to identify trusted CPs
   2. CP *may* maintain list of trusted Devices
2. Unauthenticated CP (or attacker) has only Public role unless its cert is added to ACL through introduction process
3. Remaining threats
   1. TLS renegotiation attack (fixed in initial release by prohibiting renegotiation)
   2. Malware (virus) on trusted CP
   3. Weak introduction methods (label-based PIN, push-button)
   4. Denial-of-service on initial UPnP Discovery layer
   5. Eventing layer
   6. Flaws in access control policies (of vendor or UPnP committee)
   7. Others? Please help us find them.

WANIPv6FirewallControl:1

Mika Saaranen, Nokia

Fabrice Fontaine, Orange

Mark Baugher, Cisco

Introduction

- It is expected that massive roll-outs of IPv6 will start in next couple of years
- In IPv6, we likely won’t have NATs, but it seems that business considerations require IPv6 firewalls
- There is a need to open transport addresses (pinholes) for unsolicited packets from the exterior for a duration as requested by the control point
- WANIPv6Firewall control is a service that allows hosts to:
  - Create pinholes into firewall
  - Delete pinholes
  - Check if a pinhole works (optional)

Key use cases

- Use case #1 Add pinhole
  - User has an application that needs to be contacted from the internet
  - Usually, no user interaction is needed, but application uses IGD control point to make required pinhole, but UI can be used to verify validity of request
- Use case #2 – Delete pinholes
  - Applications may remove its pinholes automatically or user may use UI to delete pinholes
- Use case #3 – find out if specified pinhole works
  - Optional feature

State variables

- FirewallEnabled : is firewall enabled
- InboundPinholeAllowed : Can pinholes be created
- OutboundPinholeTimeout : How long a pinhole created by sending traffic out remains
- And argument types for actions

Actions

- GetFirewallStatus() : returns information if the firewall is active and new pinholes can be created
- GetOutboundPinholeTimeout() : returns timeout value for automatic pinholes
- AddPinhole(): Creates a pinhole with specified arguments e.g. remote host, local host, expiration
- UpdatePinhole(): Allows extending life of a pinhole

Summary

- IGD:2 has release target in Q4/2010 including:
  - WANIPConnection:2
  - DeviceProtection:1
  - WANIPv6Firewall control:1
- Pre-published specifications are available for all UPnP Forum members

UPnP™

FORUM

For the interconnected lifestyle