Autonomic Networking Use Cases

UCAN BOF
IETF 90, July 2014

(1) Home networks

draft-carpenter-nmrg-homenet-an-use-case

Brian Carpenter

Problem statement

- Future homenets will have multiple network segments, several routers, and numerous hosts, but no expert human manager. Dedicated plug&play solutions have been proposed (HNCP etc.). The AN problem is to replace these ad hoc solutions by a generic solution that sets all necessary parameters for the homenet with minimal human intervention and without traditional top-down configuration.

Intended User & Administrator Experience

- The desired user experience is that everything just works, with no mandatory user actions, and no specialist knowledge. If any user choices are offered, there must be a reasonable default. When failures occur, recovery to the best possible running state must be automatic.
- There is no administrator.

Parameters and Information

- Parameters include trust anchor, address, prefix, routing & DNS info, identity of border devices, firewall rules,...
- Device can decide default firewall rules and RFC6724 policy
- Policy intent can include trust anchor method, non-default firewall rules, routing protocol preference, ULA yes-or-no, DHCPv6 yes-or-no, IPv4 yes-or-no,...

Interaction with other devices

- Devices need to learn/negotiate:
  - trust anchor identity
  - any non-default policies
  - identity of on-link routers
  - prefixes and addresses
  - (routers) routing protocol in use
  - (hosts) default routers and non-default address selection
  - DNS info
- Incident logging is desirable but with no administrator, it is unlikely to be used.

(2) Automatic Address Management

draft-jiang-auto-addr-management

Sheng Jiang

Brian Carpenter

Qiong Sun

Problem statement

- In large networks, prefix management still depends on human planning. Management of IPv6 prefixes and of public IPv4 addresses on AFTRs or NAT64 boxes is rigid and static after initial planning.
- The autonomic networking problem is how to dynamically and autonomically manage IPv6 address space, and public IPv4 addresses on AFTRs or NAT64 boxes, in large-scale networks, so that IP addresses can be used efficiently.

Intended User & Administrator Experience

- Normal users should see no difference.
- For administrators of a large-scale network, the management of IPv6 address space needs much less effort. Ideally, administrators just configure a single IPv6 prefix for the whole network and the initial prefix length for each device role. When sharing public IPv4 addresses on AFTRs or NAT64 boxes, administrators just configure the total available IPv4 address range.

Parameters and Information

- Parameters include: device identity, trust anchor, device role, IPv6 prefix(es) info per device, IPv4 pool per device.
- Each device can decide its own identity, role and default IPv6 prefix length.
- Policy intent includes prefix length per role, trust anchor identity, permissions (such as right to request more space), thresholds (when to request more space).

Interaction with other devices

- Information from neighbors:
  - learn which neighbors can provide more address space
  - IPv6 prefix assignment and delegations
  - IPv4 pool acquisition and sharing.
- Address usage needs to be logged for offline operations, including audit and security incident tracing.

(3) Autonomic Bootstrap

draft-behringer-autonomic-bootstrap-00

M. Behringer

M. Pritikin

S. Bjarnason

Problem/Applicability statement

- Greenfield
- Securely bootstrap new devices
  - No “leap of faith” during enrollment.
- Zero-touch
  - No pre-staging of config in new device
- Brownfield
- Distribute domain credentials
- For all market segments
- SP, ENT, IoT, Home

Problem/Applicability statement

- Secure enrollment of new devices:
  - Distribute domain credentials
  - No “leap of faith” during enrollment.
  - For Greenfield AND Brownfield
- Zero-touch bootstrap:
  - No pre-staging of config in new device
  - For Greenfield
- For all market segments
  - SP, ENT, IoT, Home

User & Administrator Experience

- Device location
  - Set up required wired / wireless connectivity
  - Power up device.
  - Walk away
- NOC (and/or any other desired location)
  - Notification of device connection
  - Add device identity to a white-list (before/after notify).
    - Ideally automated
      - bill-of-sale information.
      - Barcode scan

Parameters and Information

- Device identity
  - From manufacturing / barcode
- Domain “name”
  - Admin policy choice
- Minimum enrollment parameters
  - local EST RFC7030 server URI

Interactions / Theory of operations

- New device

  direct connection with

- Proxy registration devices

  pre-established IP connectivity (eg: ACP) with

- Registrar
  - Provides local device name, domain name, plus some parameters for the enrollment
- CA
- Cloud service (MASA):
  - The new device may receive a signed authorization token from the vendor cloud service, telling the device its target domain
- NMS: Monitoring, diagnostics, reporting

(4) Autonomic Control Plane

draft-behringer-autonomic-control-plane-00

M. Behringer

S. Bjarnason

Balaji. BL

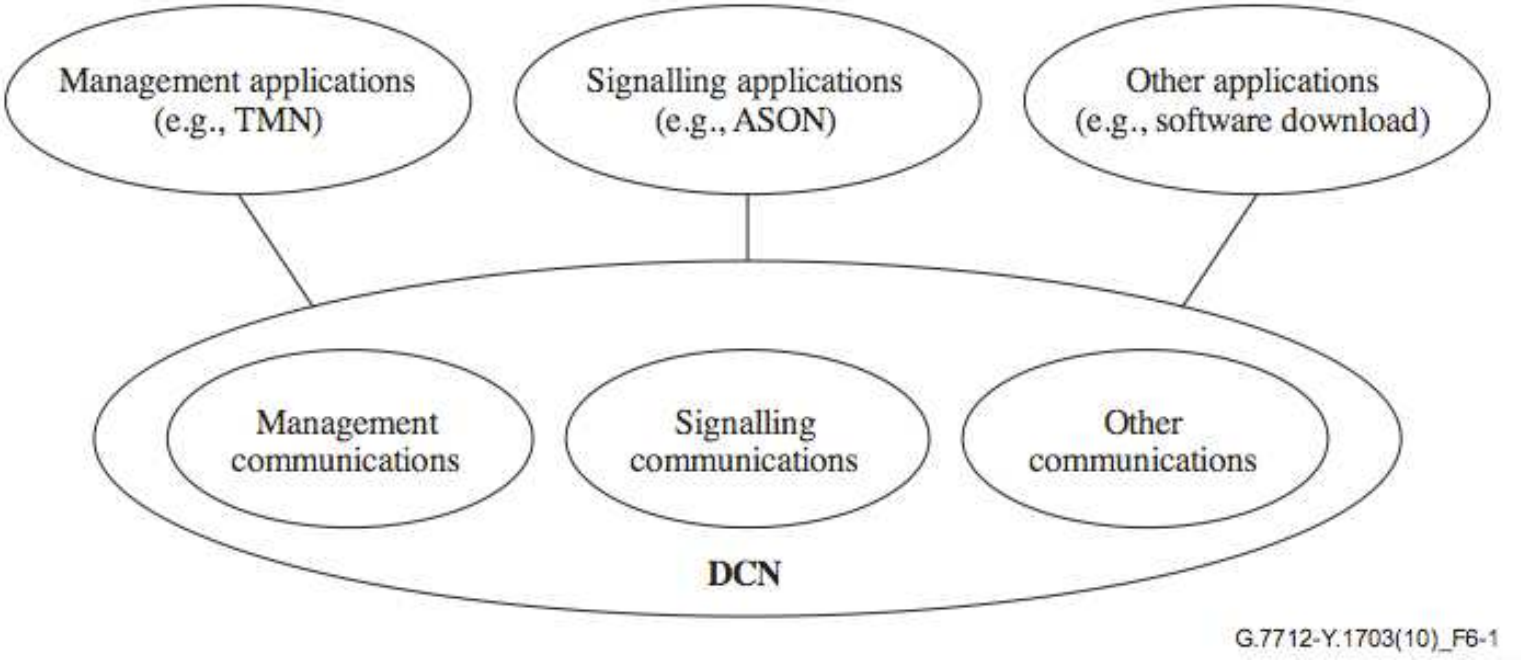
T. Eckert

Problem statement (1)

ca. 2000… G.7712/Y.1703 – DCN

Data Communications Network

Recommendation ITU-T G.7712/Y.1703 defines the architecture requirements for a data communication network (DCN) which may support distributed management communications related to the telecommunication management network (TMN), distributed control plane communications (e.g.,signalling and routing) …



Simplified english restatement: A separate physical IP network connecting to all target network equipment/devices to perform OAM for that target network without depending on that target network to operate.

Problem Statement (2)

- Network Admin/Operator
  - Get (as much as possible) benefits of DCN style network without the cost of it.
    - No additional physical equipment
    - No additional operational overhead
  - “Inband autonomic (zero-touch) DCN”
- Autonomic Network SW/Arch developer
  - Need an infrastructure on which to build higher layers of autonomic intelligence without recursive dependencies.
    - Actions of autonomic intelligence must not impact connectivity of autonomic intelligence
    - Same concern for non-autonomic intelligence (central non-autonomic provisioning).

Intended User & Administrator Experience

- User experience:

  High availability, lower cost, faster provisioning

- Administrator:

  No configuration

  Remains operational in the presence of

  - configuration errors
  - addressing or routing issues
  - Policy
  - inadvertedly affecting control plane connectivity.

- "virtual out of band channel”.

Theory of operations

- Every ACP device has a separate “small” “autonomic control plane “router” independent from the “normal” router
  - Could be a separate VRF (implementation choice)
- Every physical link between ACP devices has a secure channel for ACP to ACP communication – as independent of normal data operations as possible.
  - Eg: Ipsec/GRE over IPv6 link-local interface address
- ACP is built zero-touch, ACP configuration not changeable by OAM.
  - Routing fixed – RPL good target
- ACP used as connectivity for device bootstrap.

Parameters and Information

- Decided by device
  - Initial crypto identity
  - Link local ipv6 address
- Information from automated bootstrapping
  - Local crypto identity
  - Trust Information (e.g. domain)
- Information needed from policy intent
  - communication channel type and security type

Interaction with other devices

- Capability Negotiation
- Channel Establishment
- Routing in ACP
- monitoring, diagnostics, reporting
  - Because this is automated reporting must occur
  - Visibility of the ACP and all parameters

(5) Distributed Detection of SLA Violations

draft-irtf-nmrg-autonomic-sla-violation-detection

Jéferson Campos Nobre

Lisandro Zambenedetti

Alexander Clemm

Alberto Gonzalez Prieto

Problem statement

- Activation of active measurement probes → expensive in terms of resource consumption
  - Required resources → function of the # of measured destinations
- Better monitoring coverage → more probes
- Best practice → distribution of the available probes relying on the human administrator expertise
- Embedded management SW → deployment control
  - Network device vendors → to avoid devices starvation
  - Lack of enhancements in scalability and efficiency

Intended User & Administrator Experience

- AN solution → to avoid the human intervention
  - SLA monitoring performed by less experienced human administrators
- Some information necessary from the human administrator
  - E.g., SLOs provided by the human administrator
- Configuration and bootstrapping of network devices → minimal for the human administrator
  - E.g., information about the address of a solution-enabled device

Parameters and Information

- Each device → self-knowledge about the local SLA monitoring
  - E.g., SLOs, historical measurement data
- Devices → algorithms to decide which probes should be activated in a given time
  - AN decision of which algorithm is better for a specific situation

Interaction with other devices

- Network devices → info sharing about SL results
  - To speed up the detection and increase the # of detected SLA violations
- Local relevancy of remote results
  - Definition of network devices that exchange measurement data → creation of a new topology
- Different approaches for topology definition
  - E.g., correlated peers
  - Bootstrapping → known endpoints neighbours as the initial seed

(6) Microwave Mobile Backhaul networks

draft-bogdanovic-nmrg-mobile-backhaul-use-case-00

Dean Bogdanovic

Problem statement

- Consider bandwidth fluctuation in microwave mobile backhaul networks in routing decisions

Intended User & Administrator Experience

- Mobile backhaul network administrator will get better utilization of existing network bandwidth

Parameters and Information

- Full routing topology of MBH network
- ethernet counters on routers
- Low and high bandwidth watermarks for metric change
- Setting reference bandwith for OSPF path cost calculation

Interaction with other devices

- microwave link throughput from microwave out-door-units
- duplicate ethernet packet counters from microwave in-door-units

(7) Risk Aware Routing

draft-TBD

Laurent Ciavaglia

Bruno Vidalenc

...

Problem statement

- In case of failure, recovery mechanisms are getting involved only after a failure occurrence which cannot prevent a certain impact on traffic flows. However, there are often forewarning signs that a network device will stop working properly. Based on risk-level assessment, we can perform a proactive fault-management and isolate the failing routers out of the routed topology, and thus totally avoid detrimental impact on the service availability.

Intended User & Administrator Experience

- End users benefit from a better service experience (QoS, no/less service interruption)

- Other than formulation of *intent,* the administrator experience should not be impacted. Possible tuning/learning needed when mechanism is introduced to attain expected performance/behaviour.

Parameters and Information

- Driving parameter = risk level
  - based on hardware/software parameters monitoring

  e.g. Syslog, ACPI, SMART, traffic/load, environmental parameters (wheather, road works, cooling/power outage...)
- device can decide on reversion (risk cleared)
- policy intent: risk sensitivity/thresholds (if not learned), types of devices/areas

Interaction with other devices

- Local decision-based
  - Device information/monitoring is enough
  - Distributed execution (as per OSPF)
- Network coordination possible (FFS)
  - Potentially avoid instabilities due to local flaws
  - Deeper risk “understanding” thanks to correlation/context awareness → could lead to better overall performance/behavior
  - Sharing of local/global risk information/patterns for other mechanisms