Broadband Services

- Dual play, Triple play, Multi play
- *But what does the end-user care?*

- Nice those triple play services, but how do you get the content to the subscribers?
- Smart network architecture... and a lot of IP packets
Current broadband services over FTTH networks

- **Internet access**
  - Unicast IP (Duh...)

- **Television**
  - IP unicast for video-on-demand
  - IP multicast for broadcast television (the ‘default’ package of 50 channels)

- **Telephony**
  - SIP signaling, RTP for transport
Network Architecture – Layered model

Access
- Lots of individual connections
- Focus on physical aggregation of lines
- Security

Distribution
- Connection towards access layer
- Focus on logical aggregation of connections
- Route summarization

Core
- Connection towards the distribution layer
- Focus on traffic volume
- No identification of individual connections
Network Architecture – Layered model

Service provider 1

Service provider 2

Core network

core

metro

access
Discussion

- The how and why of current broadband networks
  - Protocols?
  - Speeds?
  - Possibilities?
  - Restrictions?
Network Architecture – Ethernet as uniform transport protocol

- ATM
- Packet over Sonet (POS)
- SONET
- SDH
- Ethernet
- X.25
- Frame Relay
- PPP
- Leased line
- STM-1, 4, 16
• “Wholesale” model: operator delivers network facilities to different content and service providers.
Network Architecture – Access: connection model

How is the connection between subscriber and network realized?

**Point-to-Point Protocol (PPP)**
- IP over PPP over Ethernet
- PPP session from the modem into the distribution layer
- IP address assignment in PPP session setup via RADIUS
- ‘connection oriented’
- Multiple PPP sessions for QoS guarantees

**Ethernet Bridging “DHCP model”**
- IP over Ethernet
- IP address assignment through DHCP
- ‘connection less’
- QoS via Ethernet Class of service
Network Architecture – Core: MPLS VPN

- Ethernet Bridging
- MPLS VPN

VPN ISP 1
VPN ISP 2
VPN ISP 3

ISP 1
ISP 2
ISP 3

CPE

subscriber domain
operator domain
service provider domain
Network Architecture – Core Network

**MPLS (Multi Protocol Label Switching)**
- Support for VPNs
- Traffic Engineering (used for fast reroute and ip multicast traffic)
- Ethernet transport over MPLS

**IP Routing**
- IGP
  - For distributing ‘next-hop’ routing information
  - OSPF or IS-IS
- M-BGP
  - For distributing IPv4 prefixes
- Label Switched Router (LSR) MPLS enabled router
- Forwarding based on Labels, forwarding control separated from forwarding plane
- Labels are distributed via Label Distributie Protocol (LDP)
- LDP hello packets are UDP and transported via broadcast of multicast
- Multiple labels (stack) per packet possible (note that MTU must be large enough!)
Network Architecture – MPLS primer: forwarding

Control plane inside a node

- IP routing protocols
- IP routing table
- MPLS IP routing control

Label information Base (LIB)

Routing information exchange with other routers

Label binding exchange with different routers

Data plane inside a node

- Forwarding Information Base (FIB)
- Label Forwarding information Base (LFIB)
Network Architecture – Increasing complexity

Complexiteit vs. Multiplay

Single play

Dual play

Triple play
What about Quality of Service?

What about Security?
Network Architecture – Quality of Service

Core network

- QoS only relevant if congestion can occur
  - Used to be irrelevant in broadband networks as bandwidth was plenty. FTTH and Docsis3 has changed this.
  - QoS policy of most providers was: “upgrade capacity”. Currently large providers are running into technological limits:
    - 10GE is not fast enough and 100GE is not yet there!
  - Cost for service providers is increasing rapidly
  - Traffic is becoming more symmetrical
Access networks

- Multi-play services all use the same connection
  - Voice traffic needs to be protected
  - Video needs to get enough bandwidth (otherwise you’ll see blocks)
- Video and voice need protection from general internet traffic (especially P2P and news traffic)
Network Architecture – Quality of Service

QoS enforcement downstream traffic

QoS parameters upstream traffic

QoS transparent

QoS parameters on incoming traffic

- IP QoS: precedence bits, diffserv
- Ethernet QoS: Class of Service (priority bit in vlan header)
- MPLS QoS: Exp. bits
Network Architecture – Security

- **Network**
  - Access to network elements
  - Access to network management systems
  - Protocols
  - “Security by obscurity”
  - Control plane protection

- **Services platform**
  - Policy: every service is responsible for its own platform
  - Where possible network security can provide additional protection

- **Separate users**
  - Spoofing filters
  - User isolation
  - Protocol filters (note that new OS like Windows Vista and 7 bring new challenges, like IPv6 default enabled).
Network Architecture – Security Attack Vectors

- ARP flood attack, plus spoofing
- DHCP flood attack
- MAC flood attack, plus spoofing
- IGMP flood attack
- IPv4 broadcast flood attacks
- IPv4 unicast flood attack
- TTL=1 attack
- IP options attack
- IPv6 MLD
- ... some others.

Focused on the control plane of the routers and switches in the network. Most are denial of service attacks, but some can be used for a ‘man-in-the-middle’ attack.
Network Architecture – Security

CPE configuration
Security \( \rightarrow \) force configuration
from a central server

(DHCP) Spoofing filters
Arp filtering

Security by obscurity
(that which is not reachable is secure)

Reverse path check
Private vlan's
vlan filtering
Network Architecture – FTTH networks Security tool box

DHCP snooping
Dynamic Arp Inspection
Private VLAN

PFC based special case
Hardware limiters

VACL Layer-2 filtering:
- Allow ethertypes 0x800 and 0x806
- Broadcast ARP filtering
- Multicast filtering
- Broadcast redirection

uRPF
Ip local proxy-arp
PIM neighbor filtering

STP filtering
ARP rate-limiting
DHCP rate-limiting
IGMP group filtering
IGMP group limiting
UUFB
UMFB
Port-security
IPSG
Storm-control

Ethertype filtering:
- 0x800 0x806 (IP & ARP)
Network Architecture – IPv6 addressing

- IPv4: address 32-bit
  - 10.100.34.123

- IPv6: address 64-bit
  - 2031:0000:130F:0000:0000:09C0:876A:130B

- IPv6 display
  - 2031:0:130F::9C0:876A:130B
  - Leading ‘0’ in a segment is optional
  - Use double colon ‘::’ to summarise two segments with 0’s allowed only once in an address.
Network Architecture – IPv6 addressing

- **Address scopes:**
  - **Unicast** – single host or interface
  - **Anycast** – group of hosts or interfaces
  - **Multicast** – group of receivers
  - There are no IPv6 broadcast addresses (!)

- **Address types:**
  - **Link-local address**, starts with FE80:: /10
  - **Site-local address**, starts with FEC0:: /10
  - **Global aggregate address**, worldwide unique
Network Architecture – IPv6 addressing

- Growth of connected networks and hosts exhausts the available IPv4 addresses → solution is IPv6
- Support for IPv6 is low
  - Most equipment is ‘IPv6 ready’ but not ‘full IPv6’
  - Performance often only about 50% compared to IPv4 performance
- (Legacy) applications usually not IPv6 ready
- Migration to IPv6 will take a long time
- IPv6 is incompatible with IPv4 (there is no implicit migration path in the IPv6 protocol design)

Network Architecture – IPv6 migration scenarios

- Dual-Stack – both IPv4 and IPv6 running on one system
  - Investments in the whole end-to-end network
  - All components must support IPv6
  - Best route to IPv6 only
- Carrier grade NAT
  - Scalability issues
- Tunneling IPv6 in IPv4
  - Scalability, and what does it solve?
- ISP world embraces Dual-Stack
- DNS is a challenge (what first? v4 of v6)
(DHCP) Spoofing filters – IPv6
Arp filtering – IPv6

CPE configuration
security → configuration envoforcement
from central provisioning system also IPv6
Quizzz

- Netwerk management?
- Why does that seem to be so difficult for most Service Providers?
Network IT - Provisioning

We like “zero touch”, “flow through” provisioning. Service providers would like to focus on “exception management” only...

Bullshit or ...?
The success of network provisioning and order management is *correct and complete information*:

- Orders
- Subscriber connections

Automation is the key, every manual action increases the chance of mistakes.
Network and IT – Systems
That’s all for now!

Questions?

Don’t hesitate to send an email to:
janmartijn @ winitu.com